FACTORI 4.0
Erasmus +

UGA
Université Grenoble Alpes

SOME CONSIDERATIONS ON CYBER-SECURITY OF CYBER-PHYSICAL SYSTEMS – INDUSTRY 4.0 CONTEXT

Jean-Marc THIRIET, Univ. Grenoble Alpes

http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/asean/asean.html

cnrs Grenoble INP UNIVERSITÉ Grenoble Alpes UMR 5216

Condensed CV

jean-marc.thiriet@univ-grenoble-alpes.fr

Docteur (Ph.D.) Université Henri Poincaré Nancy 1: February 1993

* Associate Pr. Université Henri Poincaré Nancy 1 1993-2005

* * Full Professor Univ. Grenoble Alpes since 2005

Head of the GIPSA-Lab Research Lab (April 2011-December 2015)

Research in the dependability of automation systems which integrates communication networks (Networked Control Systems) and cyber-security of cyber-physical systems (smart grids, drones)

Teaching in networks, network security, signal processing, automatic control

Education projects

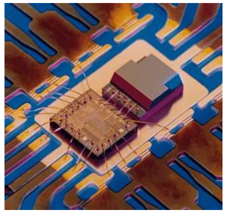
- Asean-Factori 4.0
- SALEIE: Strategic ALignment of Electrical and Information Engineering in European Higher Education Institutions

At the heart of Europe

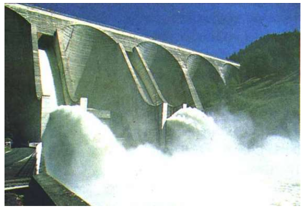
- **60,000** students
- **3,400** PhD students (45% international)
- **7,500** employees, of which
  - **5,500** academic
  - **2,000** staff
- **€ 512m** budget per year
- **82** laboratories
- **100**+ research centers
- **1** teaching hospital
- **175** hectares of campus

Copenhag
Amsterdam
London
Be
Frankfurt
Paris
Geneva
Lyon
GRENOBLE
Milan
Madrid
Rom

Some Fields of research in Grenoble (70 Research Centres)



Smart systems
Nano-techno
Energy
Water
Environment
Transportation



5 International laboratories and instruments

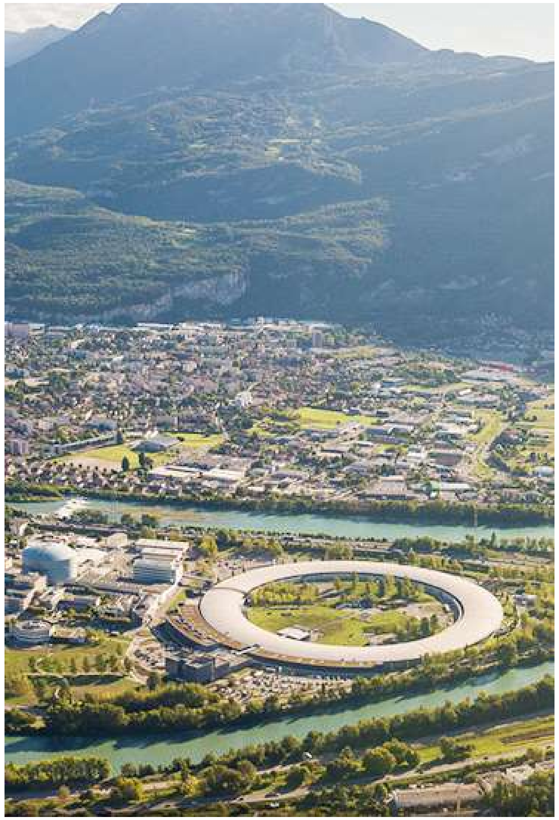
- ESRF, ILL, EMBL, GHMFL, IRAM

8 National research organizations

- CNRS, CEA, Inria, Inserm, INRAE, CRSSA, IRD, CHU Grenoble Alpes

Major companies

- Sun Microsystems, HP, Orange, STMicroelectronics, Schneider Electric, Alstom, Xerox, Thales…



Overview

1. Industry 4.0
2. PLC
3. Convergence between IT and cyber-physical systems
4. Risk analysis
5. Safety and security
6. Cyber-security
    - 6.1 Concepts
    - 6.2 Attacks
    - 6.3 Infrastructure, DMZ
    - 6.4 Cryptography and applications
    - 6.5 IDS, Virus
7. Applications to cyber-physical systems, Industrial Control Systems
8. Conclusions

1. From Industry 1.0 to Industry 4.0…

Industry 1.0 : mechanization, mechanical energy (water, steam), ex: agriculture , XIXth century

Industry 2.0 : mass production, electricity, ex: car factory ~from 1920s to 1970s

Industry 3.0 : automation (robots) => First PLCs (Programmable Logic Controllers) computer, ex: pharmacy, food, 1980

Industry 4.0 : Cyber-physical systems, communication (virtual tools: Cloud), ex: smart cities, Nowadays

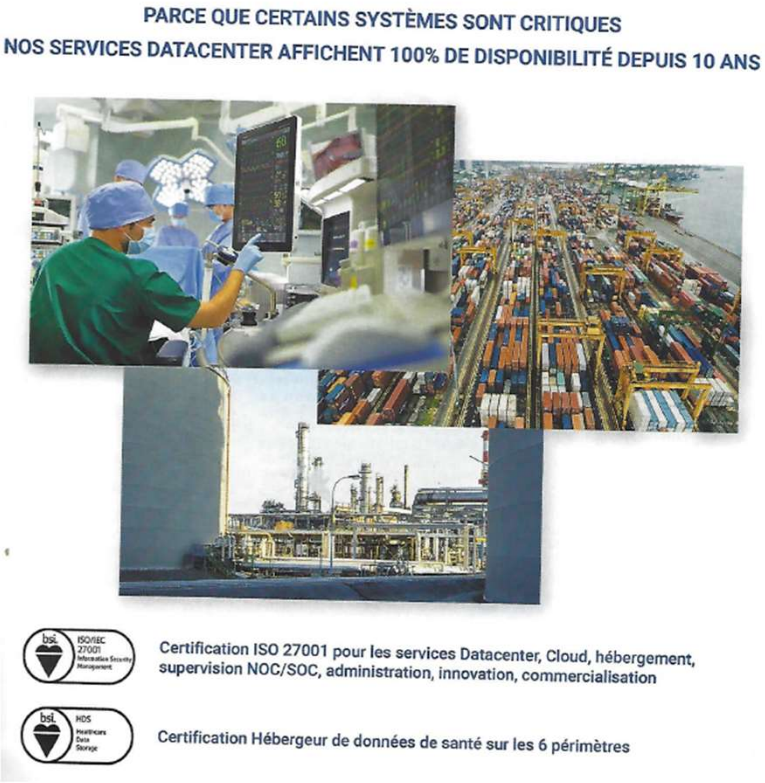
Digital twins

From Industry 1.0 to Industry 4.0…

Purposes: Production, minimal cost

- Production strategy => to product
- Maintenance strategy => to take care of the production tools
- Logistics and organization strategy => to organize production, transport and maintenance in the best way

Industry 4.0: some challenges



PARCE QUE CERTAINS SYSTÈMES SONT CRITIQUES
NOS SERVICES DATACENTER AFFICHENT 100% DE DISPONIBILITÉ DEPUIS 10 ANS

Certification ISO 27001 pour les services Datacenter, Cloud, hébergement, supervision NOC/SOC, administration, innovation, commercialisation

Certification Hébergeur de données de santé sur les 6 périmètres

Certification

Organisation

L'usine du futur devrait faire la part belle à la 5G plutôt qu'aux réseaux LPWAN. Ces derniers pourront servir cependant à l'optimisation des bâtiments.

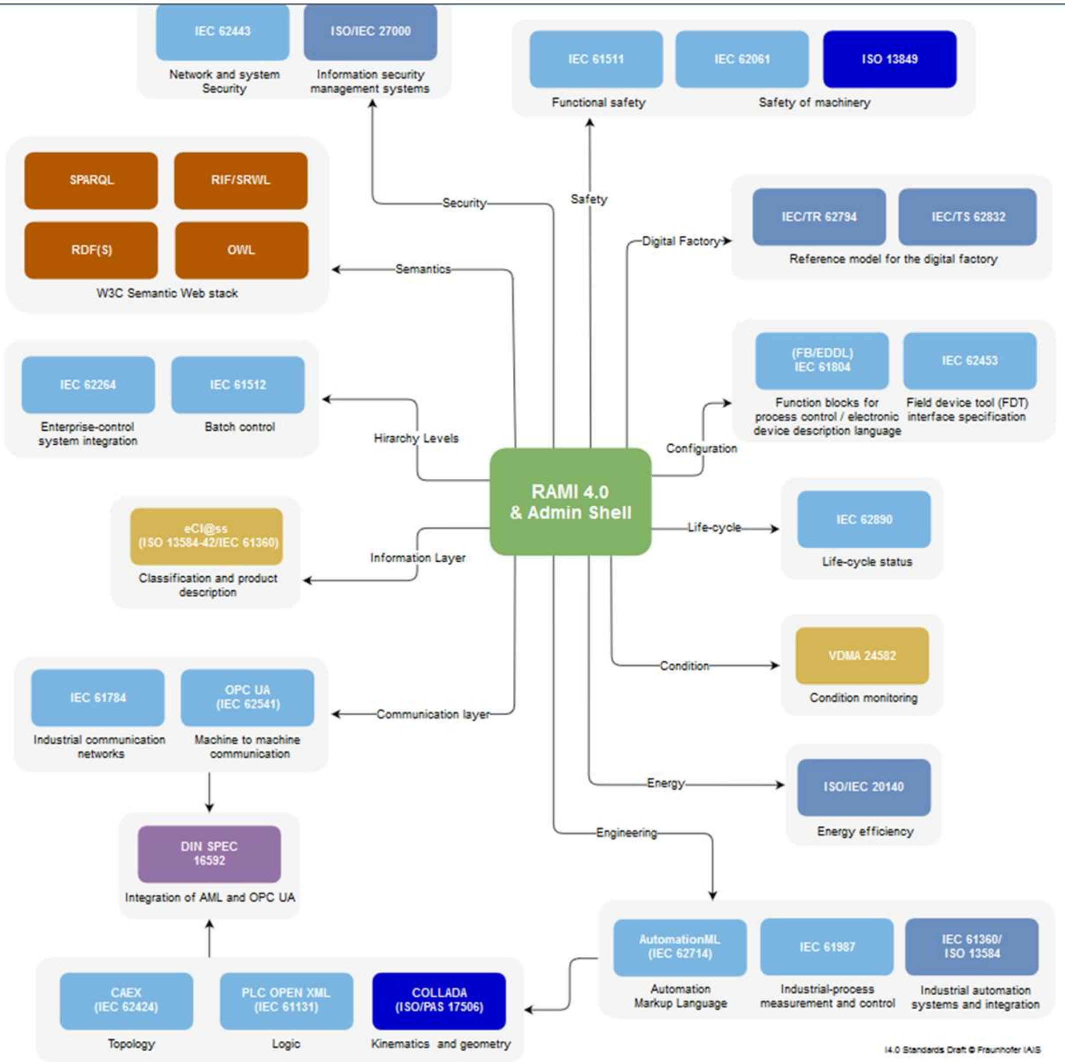
« New » networks: 5G

Certification

Standards…

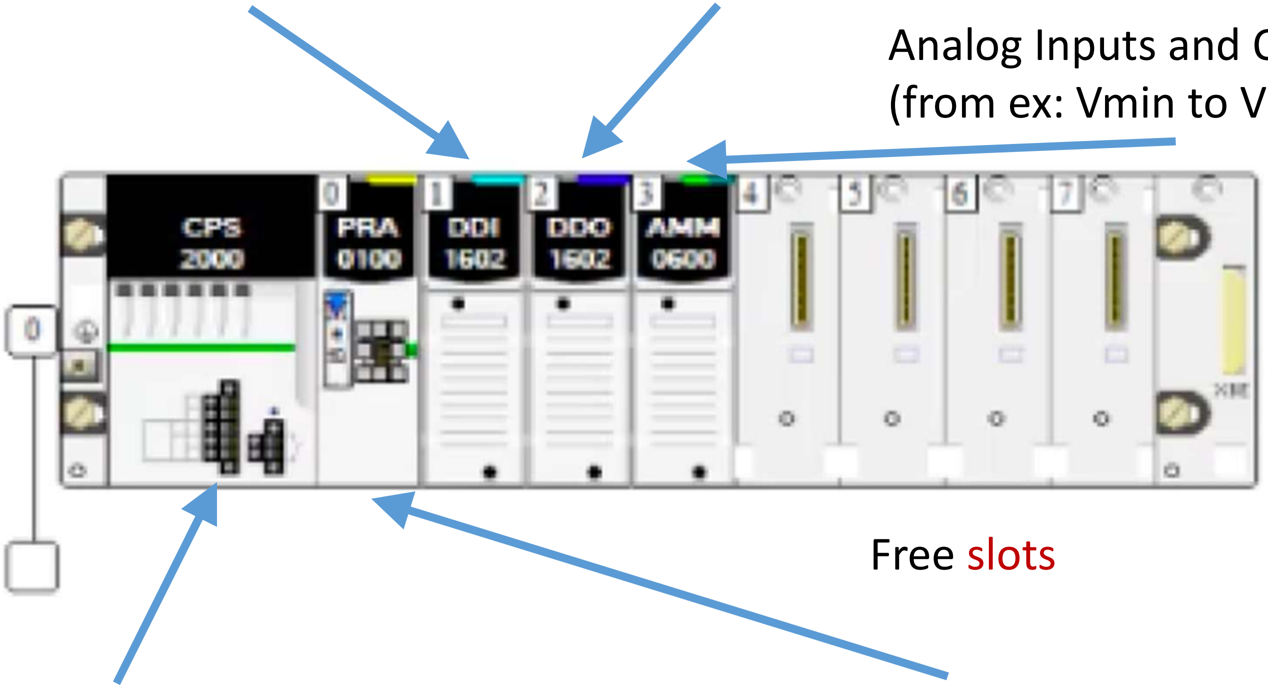
State of the Art
Best practises
In security

Quality
Assurance
processes



I4.0 Standards Draft © Fraunhofer IAIS

2. PLC (Programmable Logic Controller)



Digital Inputs (0/1)

Digital Outputs (0/1)

Analog Inputs and Outputs (from ex: Vmin to Vmax)

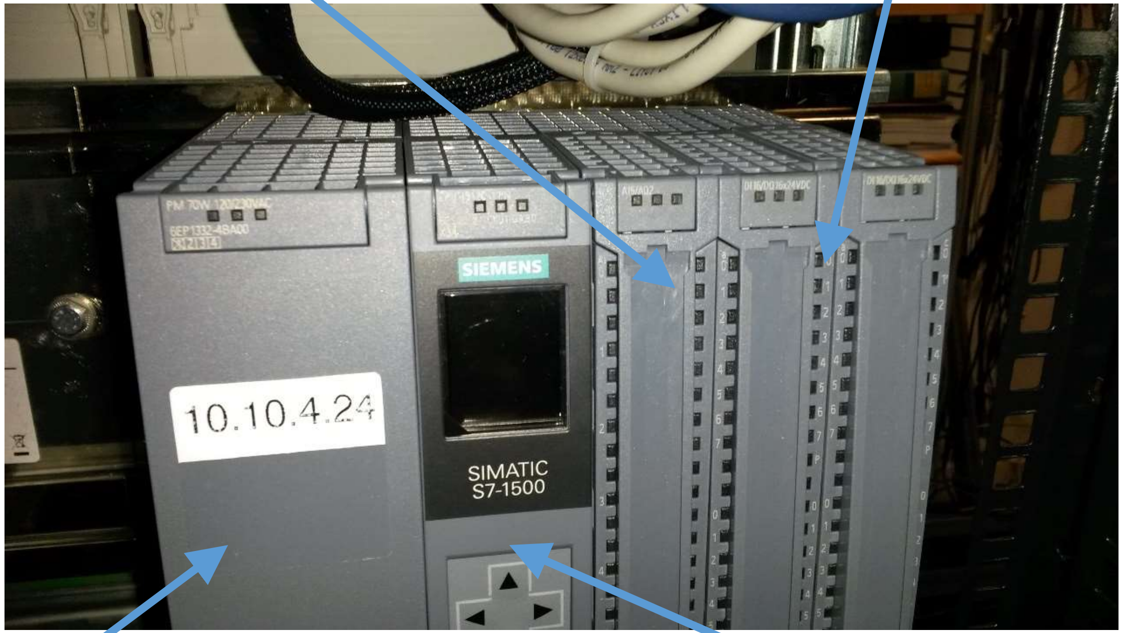
Free slots

Power Unit

Central Unit + Communication Interfaces (Ethernet and CAN (fieldbus))

Digital Inputs and Outputs

Analog Inputs and Outputs



Power Unit

Central Unit + Communication Interfaces (Ethernet and Profibus (fieldbus))

The first PLC, model 084, was invented by Dick Morley in 1969

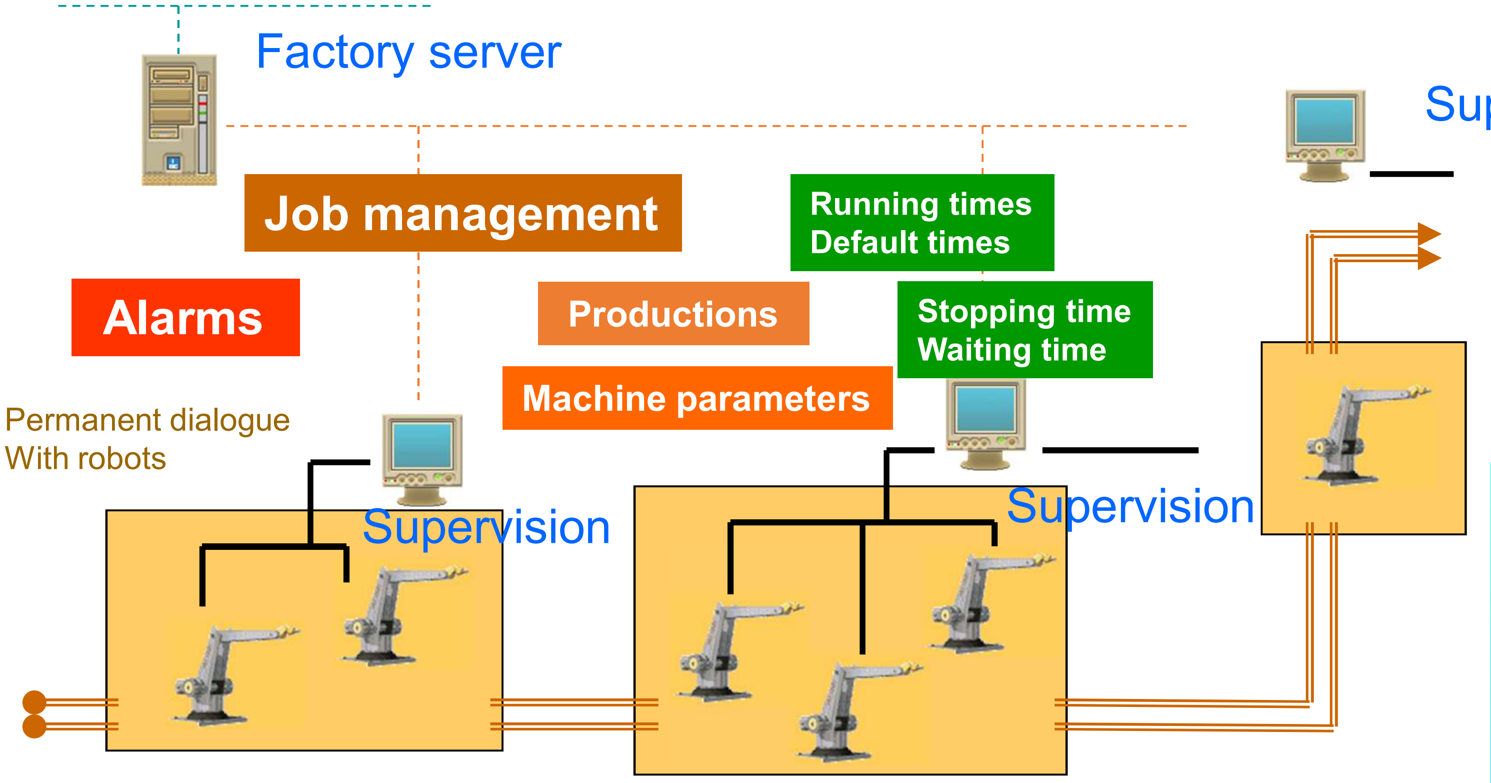
The "084" - Details

The **"084"** consisted of three major components mounted on two vertical rails, one of which was hinged to allow for service access to the front and back.

Ladder Logic:

The use of **Ladder Logic** was significant in the rapid acceptance of the **"084"** because the very same engineers and electricians who designed and maintained Factory Automation Systems could also program an **"084"**. Ladder Logic was simply an electronic version of the elementary electrical diagram that they already used -- not the case for other types of control systems being designed at the time.

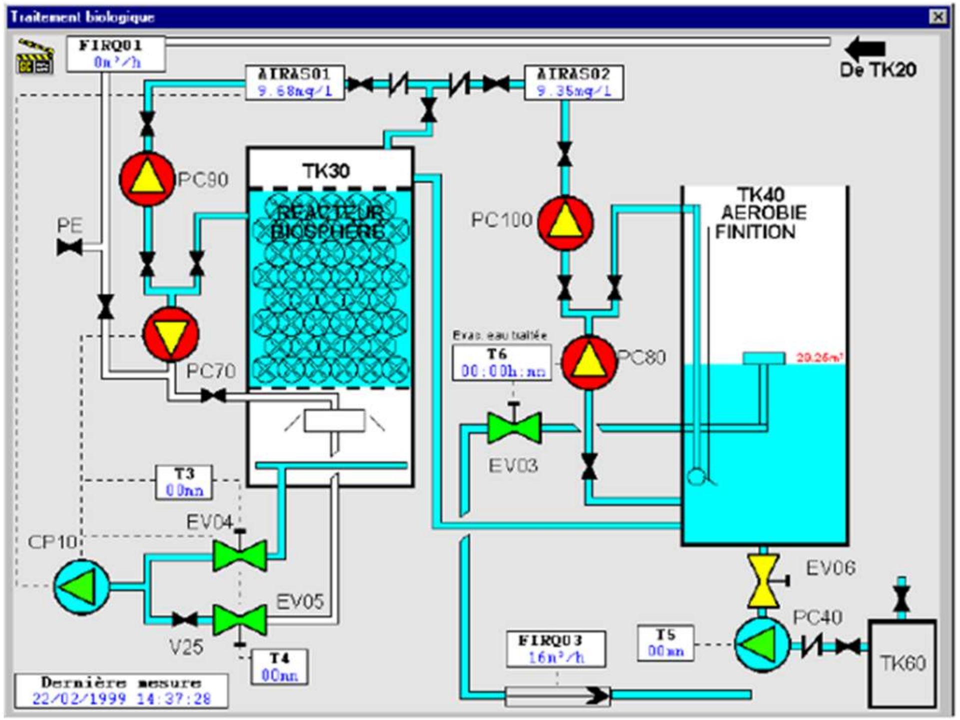
Supervision



Supervisors
Collect and process information from the robots
Basis of the factory's information system

Supervision functions

Synoptic: essential function of the supervision, provides a synthetic, dynamic and instantaneous representation of all the means of production of the unit



Traitement biologique

FIRQ01 0m^3/h

AIRAS01 9.68mg/l

AIRAS02 9.35mg/l

Evac. eau traitée T6 00:00h:mn

T3 00mn

T4 00mn

T5 00mn

FIRQ03 16m^3/h

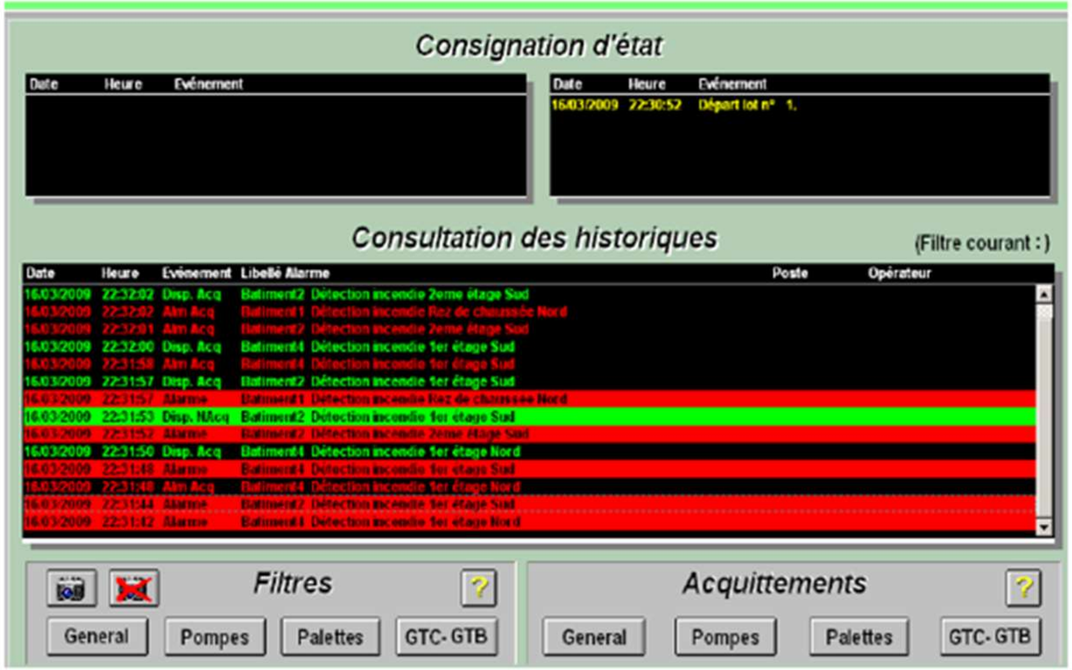
20.26m^3

Dernière mesure 22/02/1999 14:37:28

Supervision functions

Alarms

- Calculates in real time the conditions for triggering alarms
- Displays all alarms according to priority rules
- gives management tools
- ensures the recording of all the steps of the alarm processing



Consignation d'état

Date	Heure	Evénement

Date	Heure	Evénement
16/03/2009	22:30:52	Départ lot n° 1.

Consultation des historiques (Filtre courant :)

Date	Heure	Evénement	Libellé Alarme	Poste	Opérateur
16/03/2009	22:32:02	Disp. Acq	Batiment2 Détection incendie 2eme étage Sud		
16/03/2009	22:32:02	Alm Acq	Batiment1 Détection incendie Rez de chaussée Nord		
16/03/2009	22:32:01	Alm Acq	Batiment2 Détection incendie 2eme étage Sud		
16/03/2009	22:32:00	Disp. Acq	Batiment4 Détection incendie 1er étage Sud		
16/03/2009	22:31:58	Alm Acq	Batiment4 Détection incendie 1er étage Sud		
16/03/2009	22:31:57	Disp. Acq	Batiment2 Détection incendie 1er étage Sud		
16/03/2009	22:31:57	Alarme	Batiment1 Détection incendie Rez de chaussée Nord		
16/03/2009	22:31:53	Disp. NAcq	Batiment2 Détection incendie 1er étage Sud		
16/03/2009	22:31:52	Alarme	Batiment2 Détection incendie 2eme étage Sud		
16/03/2009	22:31:50	Disp. Acq	Batiment4 Détection incendie 1er étage Nord		
16/03/2009	22:31:48	Alarme	Batiment4 Détection incendie 1er étage Sud		
16/03/2009	22:31:48	Alm Acq	Batiment4 Détection incendie 1er étage Nord		
16/03/2009	22:31:44	Alarme	Batiment2 Détection incendie 1er étage Sud		
16/03/2009	22:31:42	Alarme	Batiment4 Détection incendie 1er étage Nord		

3. Convergence between IT and cyber-physical systems

003/45/784
ISAT GeoStar 45
23:15 EST 14 Aug. 2003

US Black-out, 2003

Industrial Control Systems (ICS)

Smart grids

Cyber attack ukrainian power network, Dec. 2015

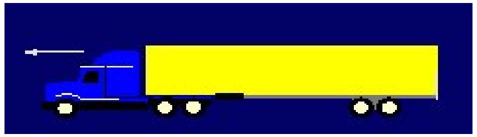
- Integrity of the information and communication infrastructure

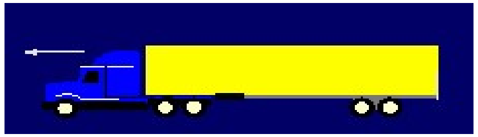
→ Challenge: DEPENDABILITY (RAMS Reliability, Availability, Security & Safety, Maintainability)

Drones
Autonomous vehicles
Connected Objects

Maroochy shire, Stuxnet, CrashOverride

Cyber-physical systems



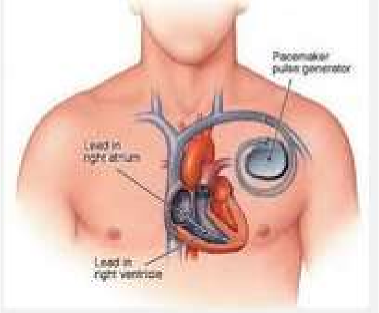


Remote-control and autonomous Vehicles

Embedded circuits
Smart devices
Embedded networks
Wireless networks
Internet of things
Ubiquitous networks
Ambient intelligence
Smart grids
Health
…

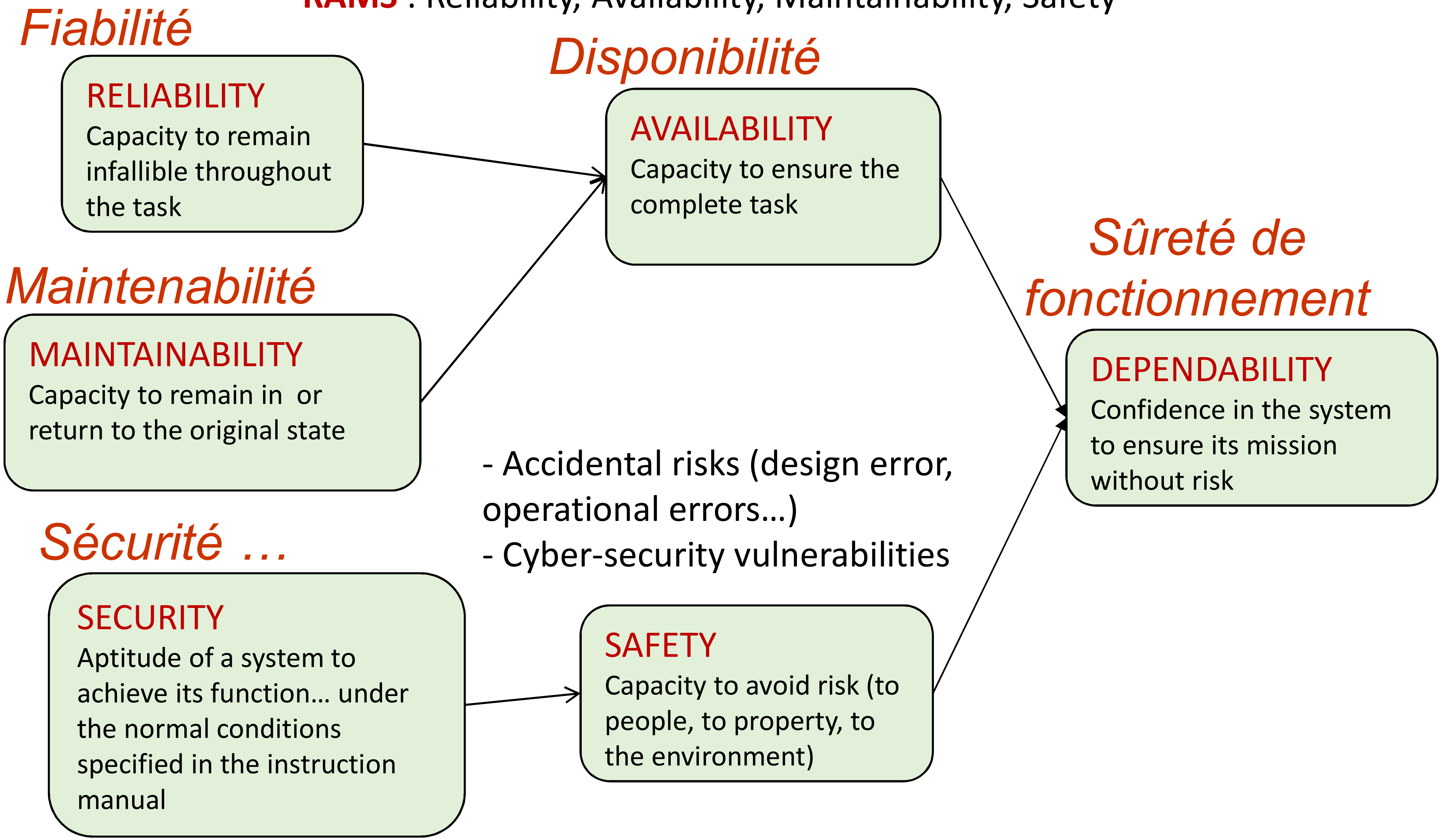
Sensor and actuators networks

Embedded systems, Internet of things



Dependability

RAMS : Reliability, Availability, Maintainability, Safety



Fiabilité

RELIABILITY
Capacity to remain infallible throughout the task

Disponibilité

AVAILABILITY
Capacity to ensure the complete task

Maintenabilité

MAINTAINABILITY
Capacity to remain in or return to the original state

Sûreté de fonctionnement

DEPENDABILITY
Confidence in the system to ensure its mission without risk

- Accidental risks (design error, operational errors…)
- Cyber-security vulnerabilities

Sécurité …

SECURITY
Aptitude of a system to achieve its function… under the normal conditions specified in the instruction manual

SAFETY
Capacity to avoid risk (to people, to property, to the environment)

4. Safety = RISKS ANALYSIS => Risk Management

To Identify failures in a more exhaustive manner

- Crashing of hardware disks
- Burning down, or flooding of premises containing backups
- Open ports on a network

To evaluate the severity of each failure (level of risk)

To envisage the failures (use of evolution models)

- 'Outdatedness' of the data-processing components
- Probability of attacks by third parties on vulnerable ports

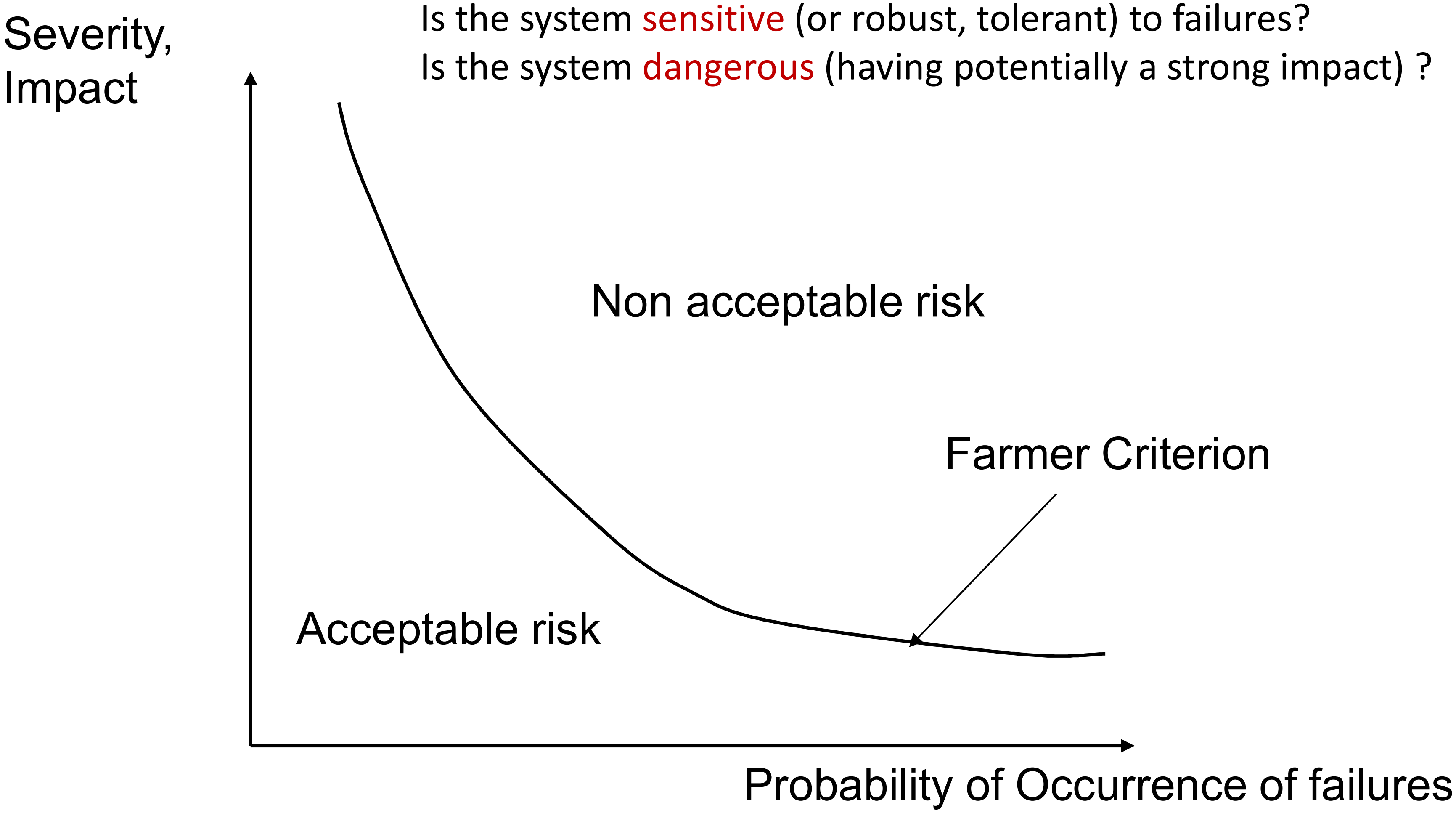
At each **observation** of a failure, we should associate the appropriate **measurement** (statistical) => to improve the forecasting models

To control the failures

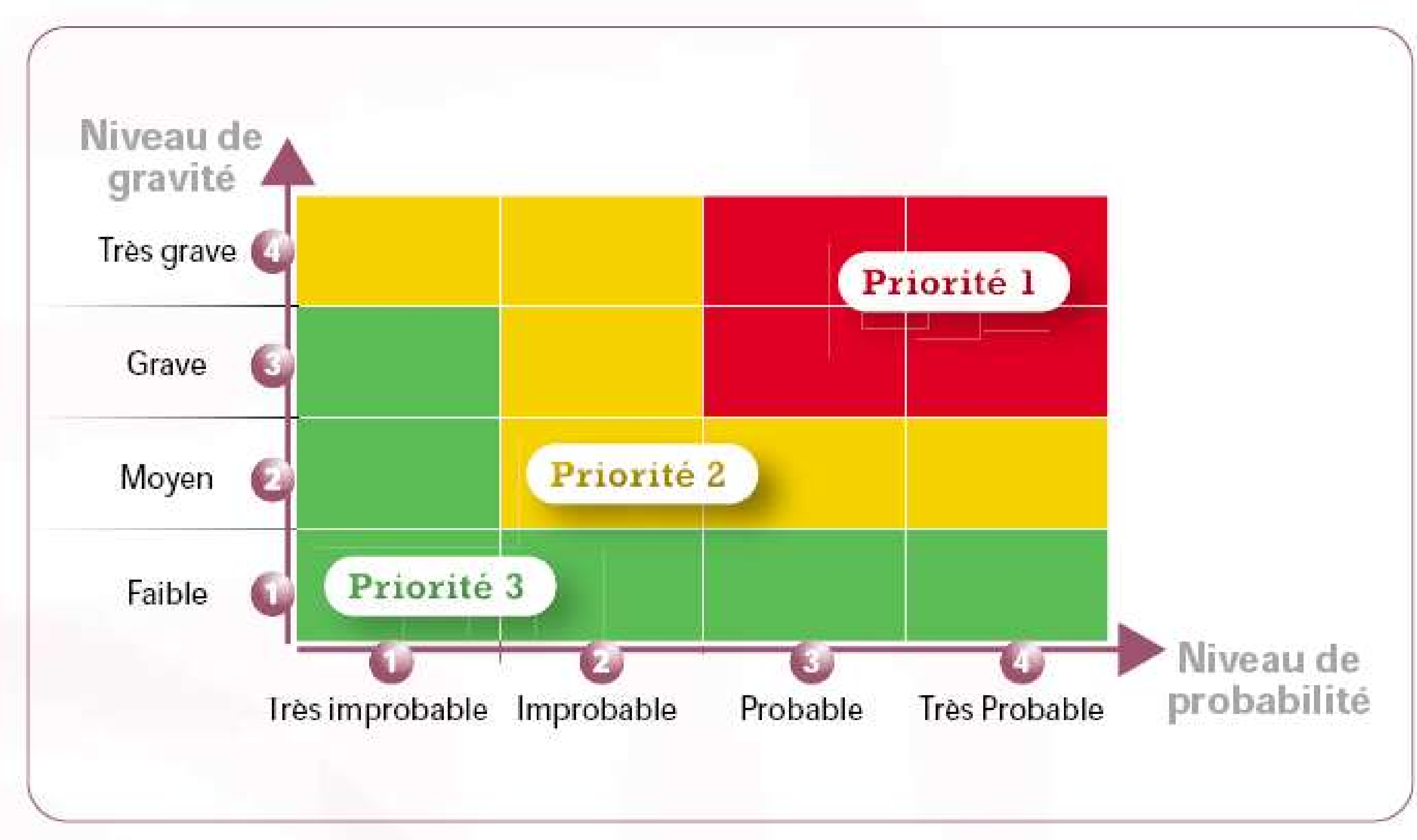
- Reduction of their frequency
- Preventive measures against the consequences (reduction of the impact)
- Tolerance

Risk analysis: Severity-probability

Is the system sensitive (or robust, tolerant) to failures?
Is the system dangerous (having potentially a strong impact) ?



Risks evaluation, evaluation of the severity



Example

Danger (cause)	Dangerous situation	Dangerous event	Risk of…	Consequence	Severity	Probability	Priorities	Observations
Explosion of a tyre	Car sliding	Screw in the tyre	Accident	Killing people in the car	4 (high)	1 (low)	1 (low)	Having a spare wheel…

Prescriptions, Methods for risk analysis

Methods

1. FMEA (Failure Mode and Effect Analysis)/AMDE
2. HAZOP (Hazard and Operability Study)
3. Preliminary Hazard Analysis
4. MEHARI (Method for Harmonized Analysis of Risk) (FR, CLUSIF)
5. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité, FR, ANSSI)
6. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation, US-CERT)
7. CRAMM (CCTA Risk Analysis and Management Method, UK CCTA (Central Communication and Telecommunication Agency))

Prescriptions

1. US standard NERC-CIP-002-3 Critical Cyber Asset Identification
2. US standard NIST.IR 7628 Guidelines for smart gris security
3. ISA/IEC 62443 Security for Industriel Automation and Control Systems
4. EU efforts about smart grid security
5. ANSSI Classification method and key measures

5. Safety and security: definitions

- Security: definition (from EN 292 standards)

  Aptitude of a system to achieve its function… under the normal conditions specified in the instruction manual…

- Safety

  Aptitude of an entity to avoid revealing critical or catastrophic events => likely to affect people, equipment, the environment

- **Confidentiality & Integrity**

  Aptitude of one entity to safeguard the confidentiality and the integrity of information

6. Security

UMR 5216

6.1 Definitions of terms related to the reliability and the security for applications such like data- processing networks (1/2)

Direct Properties of Security

- Confidentiality (*confidentialité*): preventing the visualization of information by unauthorized persons

- Integrity (*intégrité*): preventing the non-detection of modifications of information by unauthorized persons

- Authentication (*authentification*): allowing the identity check of users

Property linked to security

- Availability (*disponibilité*): *preventing* unauthorized persons access in order to guaranty the use by authorized users

Definitions of terms related to the reliability and the security for applications such like data- processing networks (2/2)

- Authorization *(autorisation)*: preventing access to the system by unauthorized persons

- Auditability *(auditabilité)*: possibility of rebuilding the complete history of the system from recordings of histories

- Non “repudiability” *(non répudiabilité)*: possibility of providing irrefutable proof of the perpetrator of an action on the system

- Protection from third parties: preventing serious damage linked to an attack (pirating) by third parties.

Security principles

- Physical security
  - Energy sources (electricity (power supplies)…)
  - Environmental protection (fire, temperature, moisture/fungi/fungus (humidity)…)
  - Protection of access, traceability of accesses
- Exploitation security
  - Back up plan, recovery plan
  - Emergency help plan
  - Management of the computer park, configurations and updates
  - Management of the incidents and follow-ups until resolution
  - Analysis of accountancy and logging files
  - Management of the maintenance contracts
- Logical security
  - Mechanisms of security by software: Identification, Authentication, Authorization
  - Cryptography mechanisms
  - Effective password management
  - Antivirus
  - Classification of data: Degree of sensitivity (normal, confidential…)
- Applicative security
  - Development Methodology (respect of the development standards suited to the technology employed)
  - Programmed checks, tests
  - security of the software packages (choice of the suppliers, interfaces security)
  - Contracts with subcontractors (responsibility clauses)
  - Migration plan of critical applications
  - Validation and audit of programs

6.2 Types of targets, types of attacks

STUXNET

Convenient target *(cible opportune)*

-By “chance”: detected by the pirates in the search of least protected machines or servers

-What to do?: update the systems

-To test the system (try to find faults)

Chosen target *(cible de choix)*

-Precise Target: strategic interest of the company …

The types of attacks are classified in two categories:

Passive attacks

- Interception, listening

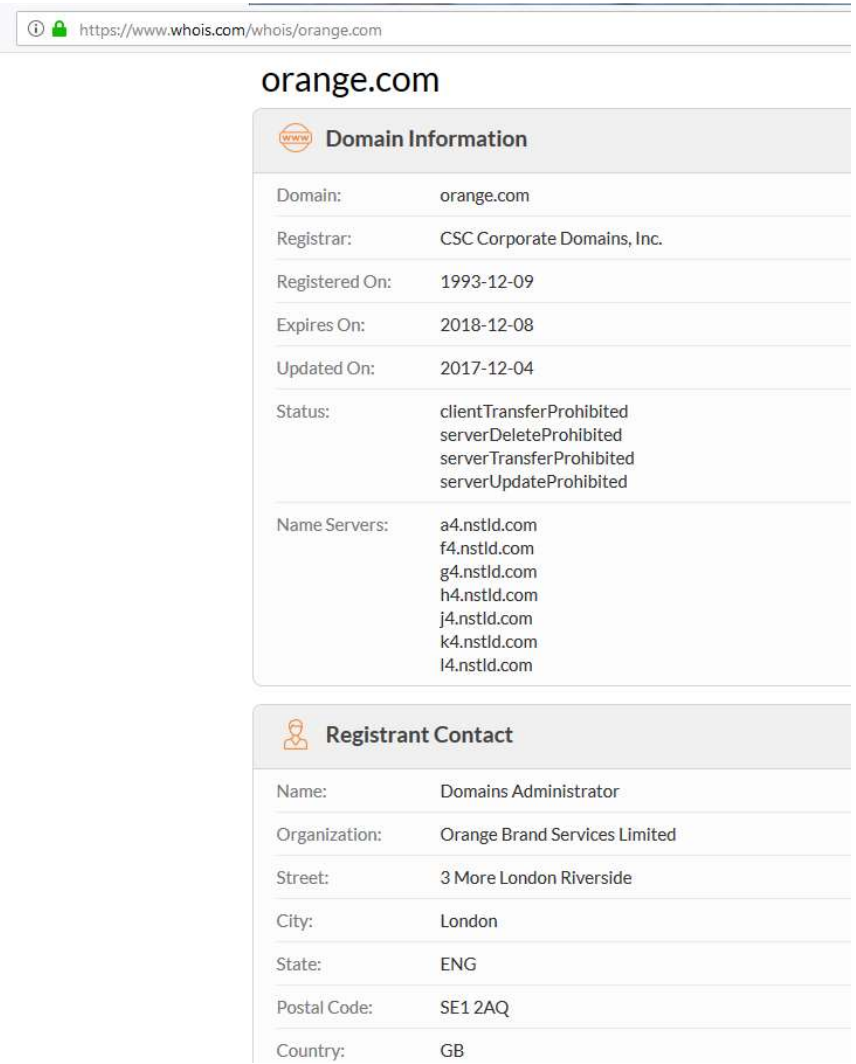
Active attacks

- Modification
- Interruption
- Denial of service

In-depth security

Attacks 1/6: Recognition and collection of information

- Domain names, DNS servers, blocks of assigned IP addresses
- IP addresses accessible from outside
- Services presenting a valid target
  - www, ftp, e-mail…
- Types of machines on which the services are carried out
  - Operating systems and number of version => use of the exploitable known faults
- Type of firewall and IDS (Intrusion Detection System)
- User names, groups, routing tables, SNMP information
- Physical location of the equipment and systems
- Used network protocols (IP, IPv6, IPSec, SSL/TLS)
- Cartography of the network
- Type of access connections
  - Traditional access (frame relay, broad band)
  - Wi-Fi Access
- Approach by “social engineering” (consists in questioning people and recovering information by trapping them)
  - Information on the people, their names, telephone numbers, situation in the company, addresses…



https://www.whois.com/whois/orange.com

orange.com

Domain Information

Domain:	orange.com
Registrar:	CSC Corporate Domains, Inc.
Registered On:	1993-12-09
Expires On:	2018-12-08
Updated On:	2017-12-04
Status:	clientTransferProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	a4.nstld.com f4.nstld.com g4.nstld.com h4.nstld.com j4.nstld.com k4.nstld.com l4.nstld.com

Registrant Contact

Name:	Domains Administrator
Organization:	Orange Brand Services Limited
Street:	3 More London Riverside
City:	London
State:	ENG
Postal Code:	SE1 2AQ
Country:	GB

Attacks 2/6: Scan of the services and the ports

- Detailed Scan of a target (NMAP = Network Mapper)

Attacks 3/6: Enumeration

- Extraction of information on the valid accounts and the resources

  Network resources and shared resources

  Users and groups (as a function of the Operating system)

  Applications

  Character strings sent in response by the equipment

Attacks 4/6: Obtaining an access

- Tackle at the operating system level

  Use of the functionalities of the O.S.

- Tackle at the application level

  Use of the functionalities of the application

- Attack benefiting from a bad configuration

  "Opened" system, default configuration (administrator name and password!), many activated functionalities

- Attack using lodged scripts

  Scripts available on the system and sometimes activated by default (Unix/Linux)

  Détournement de requêtes SQL lors de l'interrogation d'une base de données via interface web

- Automated Attack (ex: scan of port 80 of a whole C-class block of addresses in order to seek a fault)

- Targeted Attack : much rarer but difficult to detect (experienced pirates)

Attacks 5/6: Extension of the acquired privileges

If the pirate succeeded in entering on the system with a “weak” password => extension of the rights (authorizations)

- To carry out code to obtain privilege
- To seek to decipher other passwords
- To scan for non ciphered passwords
- To seek possible inter-network relations
- To identify badly configured files or shared resources permissions

Attacks 6/6: Cover the traces

To dissimulate to the administrator the fact that one penetrated the system

-Windows: To eliminate the entries (inputs) in the event logs and the registers

-Unix: to empty the file of history (execution of the program *log wiper*)

-! The attacker cleans the log files but does not remove them!

Attacks types

Deny Of Service DOS

Sniffing, to get information

Scanning, to get information

Social engineering

Cracking

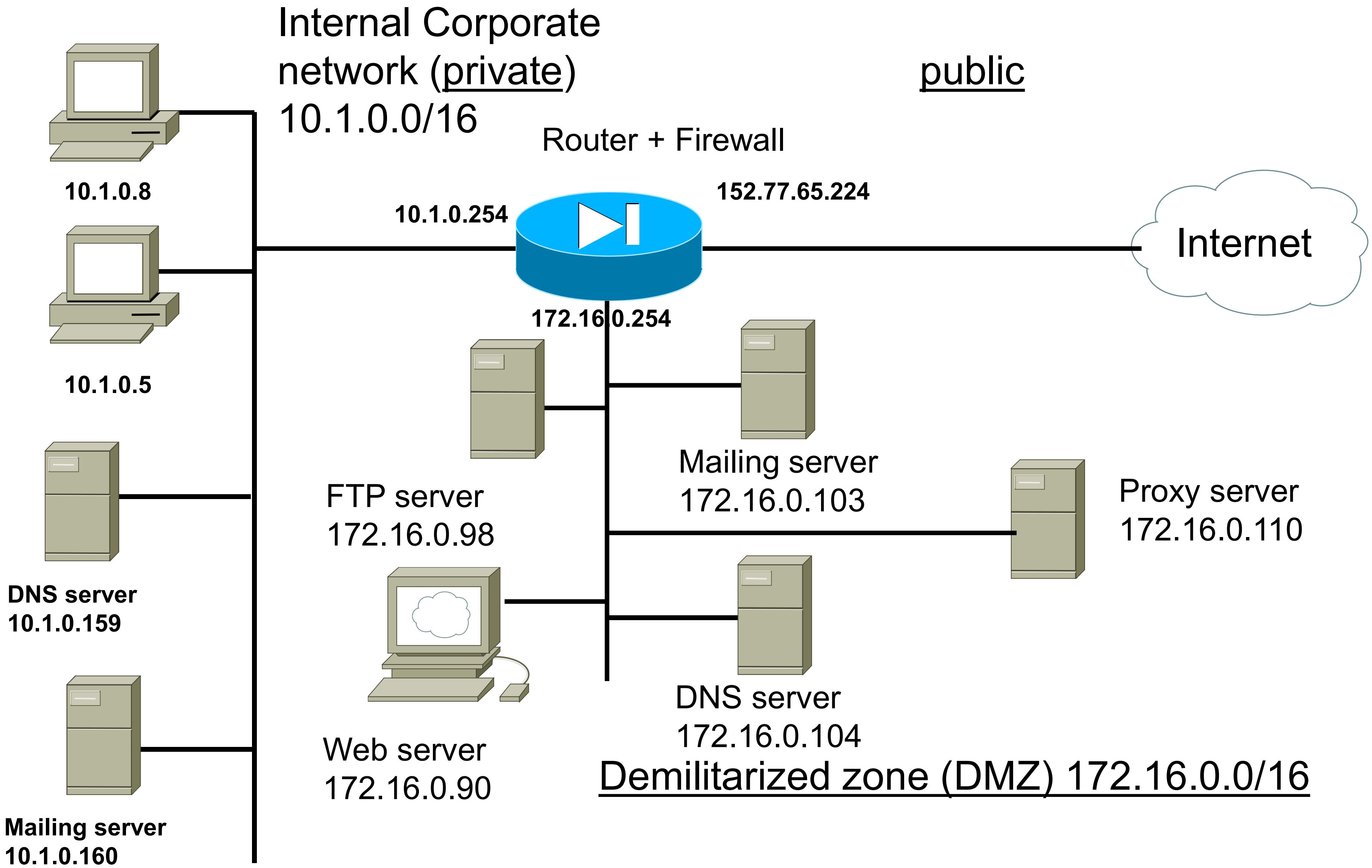
Spoofing, to remote-control the process,

Man in the middle

Hijacking

Buffer overflow

6.3 A network…


Internal Corporate
network (private)
10.1.0.0/16
public
Router + Firewall
10.1.0.8
10.1.0.254
152.77.65.224
Internet
172.16.0.254
10.1.0.5
Mailing server
172.16.0.103
FTP server
172.16.0.98
Proxy server
172.16.0.110
DNS server
10.1.0.159
DNS server
172.16.0.104
Web server
172.16.0.90
Demilitarized zone (DMZ) 172.16.0.0/16
Mailing server
10.1.0.160

Stateful firewall: Dynamic Access Control List

Dynamic filtering

- **Stateful inspection firewall**: packet filters that take into consideration OSI-layer 4 (TCP, UDP)
- Dynamic entries for responses to the TCP, UDP, ICMP requests
- Does not require to keep open the static ports (the ports remain open only during the time of the session)

Follow-up/monitoring of the TCP sequence numbers

- Monitoring of the sequence numbers of the input and output packets to follow-up communication flows
- Protection against “man in the middle” attacks and session hackings

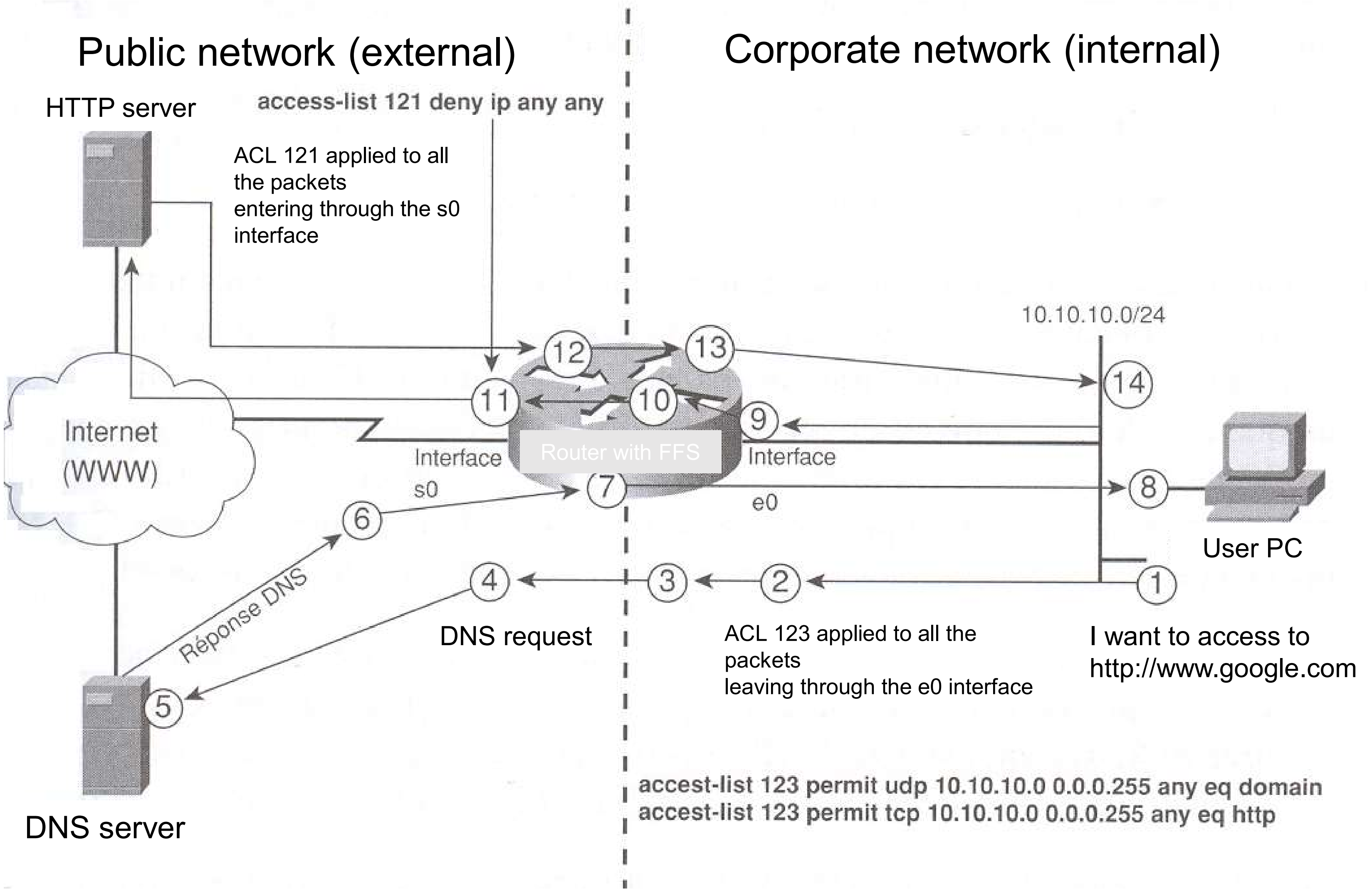
Ex: 121 ACL applied to router input, from Internet to LAN

Action Prot Adr. S. Adr. D. Serv./Port

```
ip address 192.168.254.1/30
ip address group 121 in
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any unreachable
access-list 121 permit icmp any any administratively-prohibited
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14.61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```

1 action: permit/deny
4 parameters

Example



Public network (external)

Corporate network (internal)

```
access-list 121 deny ip any any
```

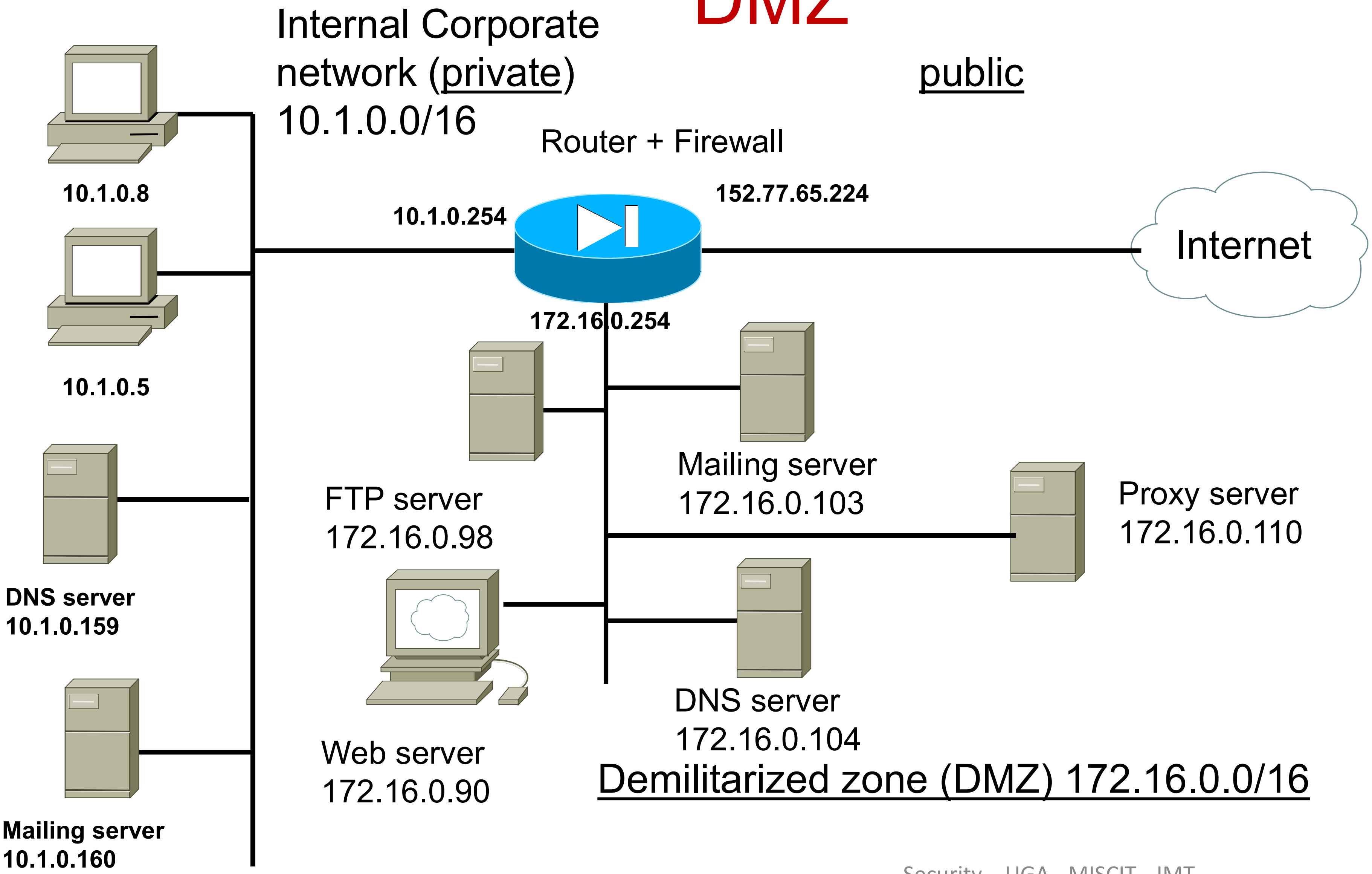
ACL 121 applied to all the packets entering through the s0 interface

ACL 123 applied to all the packets leaving through the e0 interface

I want to access to http://www.google.com

```
accest-list 123 permit udp 10.10.10.0 0.0.0.255 any eq domain
accest-list 123 permit tcp 10.10.10.0 0.0.0.255 any eq http
```

A network with a firewall/router… DMZ



Exercise 1

- We use a stateful firewall
- The machines from the inside network should be able to reach any machine in the DMZ or outside (for the mail)
- The machines from the DMZ should be able to reach any machine outside BUT NOT inside (for the mail)
- Concerning http
  - Any machine from inside should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
  - Any machine from the DMZ should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
  - The proxy should be able to reach any http server (port 80) everywhere
- We should not forget the DNS aspects (port 53)

Exercise 1

- We use a stateful firewall
- The machines from the inside network should be able to reach any machine in the DMZ or outside (for the mail)
    - Access-list 1 permit mail 10.1.0.0/16 any eq 25
- The machines from the DMZ should be able to reach any machine in outside BUT NOT inside (for the mail)
    - Access-list 1 deny mail 172.16.0.0/16 10.1.0.0/16 eq 25 (should be before !)
    - Access-list 1 permit mail 172.16.0.0/16 any eq 25
- Concerning http
    - Any machine from inside should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
    - Access-list 1 permit tcp/udp 10.1.0.0/16 172.16.0.110 eq 3128
    - Any machine from the DMZ should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
    - No rule
    - The proxy should be able to reach any http server (port 80) everywhere
    - Access-list 1 permit tcp 172.16.0.110 any eq 80
- We should not forget the DNS aspects (port 53)
    - Access-list 1 permit tcp/udp 10.1.0.159 172.16.0.104 eq 53
    - Access-list 1 permit tcp/udp 172.16.0.104 a_specific_DNS_Server_outside eq 53
    - Access-list 1 deny any any any eq any

Some considerations on security for CPS

Everything which is not explicitely authorized is forbidden by default

In depth-security

- Global vision of the security strategy and implementation (not a juxtaposition of security mechanisms…)
- Security everywhere (internal, external)
- Application-oriented firewall

Some issues of security

- Organisational approach (security policy, human aspects, saving policy, management of users)
- Methodological approach (firewall configuration, attacks strategies and defense…)
- Technological approach (network, topology, servers, hardware and software firewalls, security protocols)
- Theoretic approach (cryptology, virology)
- Testing (quality) approach (checking, testing, audit…)

Question of implementation on low-resource embedded systems

6.4 Some issues of cryptography

To guarantee as well as possible

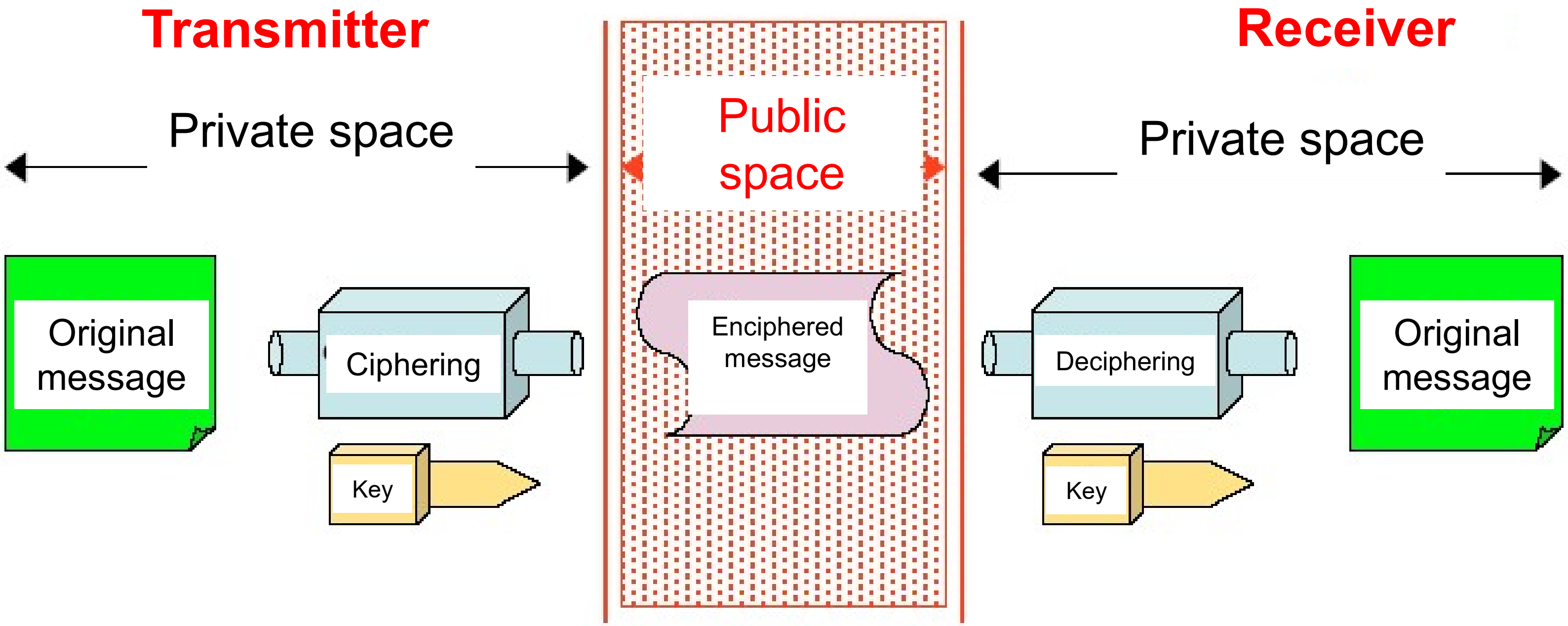
- Confidentiality
- Authenticity
- Integrity

of data (or information) exchanged

Two strategies

- Symmetric cryptography
- asymmetric cryptography
- Hybrid cryptography

Symmetric Cryptography (*common, shared* secret key)



- ✓ The same key is used for enciphering and deciphering
- ✓ Problem: how to transfer the key

Size of the key

- Key enciphered on n bits => 2^n values
- The longest is the key
  - The most important is the number of possible keys
  - more time is necessary to compute and find the result
- A 40 bit-key (10^{12} different possibilities) => it has become now rather simple to break them
- Significant information => prefer a 128 bit-key (10^{38} possibilities) or a 256 bit-one
- Note: it is easier to find the key from a user or from the storage system than to find it thanks to deciphering

Size of the key…

Knowing that a specific computer (“DES cracker” in 1997) needs on average 4,5d to “crack” a 56-bit key through an exhaustive search (brute force attack). For the next questions, please give the answer in the relevant time unit

How long would it take to find a 40-bit key?

How long would it take to find a 112-bit key?

Size of the key…

Knowing that a specific computer (“DES cracker” in 1997) needs on average 4,5d to “crack” a 56-bit key through an exhaustive search (brute force attack). How long would it take to find a 40-bit key?

$$4{,}5 * \frac{2^{40}}{2^{56}} = 4{,}5/2^{16} = 4{,}5/65536 = 6{,}87.10^{-5}\ jours = 5{,}93s$$

How long would it take to find a 112-bit key?

$$4{,}5 * 2^{112-56} = 4{,}5 * 2^{56} = 2{,}88.10^{17}\ jours = 7{,}89.10^{14}\ ans$$

which means approx. 60 000 Big Bangs (1 BB = 15.10^{19} years)

Robustness of the enciphering system

- Power of the algorithm (non-secret algorithm)
- Size of the key used
- Capacity to keep the secret keys in a protected way
- A system of enciphering is known as reliable, robust, sure, protected if it remains inviolable independently of the computing power or time available to an attacker
- It is known as operationally protected (*computational secure*) if its security depends on a series of realizable operations in theory, but unrealizable practically (too long processing times…)
- It is necessary to frequently change the enciphering key

Symmetric cryptography: Caesar ciphering

Replacement of a letter by another

Robustness?

- Identical frequency contents
- Can be easily "broken" easily starting from a message of 28 letters…

Example: shift of two letters towards the line

- *Bonjour* => Dqplqwt

Another example: shift of a letter towards the left

- IBM => HAL ("2001: A Space Odyssey")

Symmetric cryptography: poly-alphabetical codes

- Let’s consider an alphabet {A, B, C, D}

text t key k	A B C D
A	C D B A
B	D C A B
C	C A B D
D	B D A C

plaintext: ABCB ACCB AACB B

Key: DBBC BAAC DDBB C

Encrypted text: BCAA DBBA BBAC A

- Require very large size keys not to be very vulnerable …

Symmetric cryptography: Operations at the bit level Distance permutations

XOR functions

- d1=1, d2 = 01, d3 = 001, d4= 0001…
- Distance permutation (di, dj)
- Example: TS
- Form substitution
- Example (d1, d2, d3, d4) substituted by (d2d3, d3d1, d1d4, d1d3) => increases the size of the data

TS

54 53

0101 0100, 0101 0011

d2 d2 d2 d4 d2 d3 d1

d3d1 d3d1 d3d1 d1d3 d3d1 d1d4 d2d3

0011 0011 0011 1001 0011 10001 01001

What is the size of the original message? The encrypted one?

- Then to decipher…

Symmetric cryptography: Operations at the bit level Distance permutations: exercise

- Encipher *BON* by substituting (d1, d2, d3, d4, d5, d6) by (d2d3, d3d1, d1d4, d1d3, d2d4, d5d6) with d1=1, d2 = 01, d3 = 001, d4= 0001…

BON

What is the size of the original message? The encrypted one?

42, 4F, 4E

Example

- Substitution (d1, d2, d3, d4, d5, d6) by (d2d3, d3d1, d1d4, d1d3, d2d4, d5d6)
- 42, 4F, 4E
- 0100 0010   0100 1111   0100 1110
- Encoding
- d2   d5   d3 d3 d1d1d1 d2 d3d1 d1, ! 0 is not taken into account…
- Encryption
- d3d1 d2d4 d1d4 d1d4 d2d3d2d3d2d3 d3d1d1d4 d2d3d2d3
- 0011 010001 10001 10001 010010100101001 001110001 0100101001
- What is the size of the original message? The encrypted one?
- 24 bits (3 bytes) for the original message, 54 bits for the encrypted one

Symmetric cryptography: Inversion of bits according to a random suite

$(a_n) = (2, 14, 7, 11, 74, 25, 32, 37, 152, 99, 7)$

$\Rightarrow (b_n) = (2, 6, 7, 3, 2, 1, 0, 5, 0, 3, 7)$

F= 01001010 10010101 00101001 00010100 11010110 11110001

And

F'= 01**1**010**01** 100**0**0101 00**0**01001 0**1**010100 **0**1010**0**10 **0**11**0**000**0**

Bit 2 Bit 6 Bit 3 Bit 2…

Symmetric cryptography: Inversion of bits according to a random suite: exercise

BON with the random suite

(a_n) = (3, 4, 11, 27, 32, 25, 12, 153, 77, 7)

We work on 8-bit packets

42, 4F, 4E

Inversion of bits according to a random suite : example 2

- *BON* with the random suite (a_n) = (3, 4, 11, 27, 32, 25, 12, 153, 77, 7) modulo 8
- 42, 4F, 4E
- 01000010 01001111 01001110
- (b_n) = (3,4,3,3,0,1,4,1,5,7)
- 01011010 01011111 01011110

Symmetric cryptography: The standard algorithm for enciphering: IBM DES (Data Encryption Standard)

Created 1977

At first for classified or secret documents

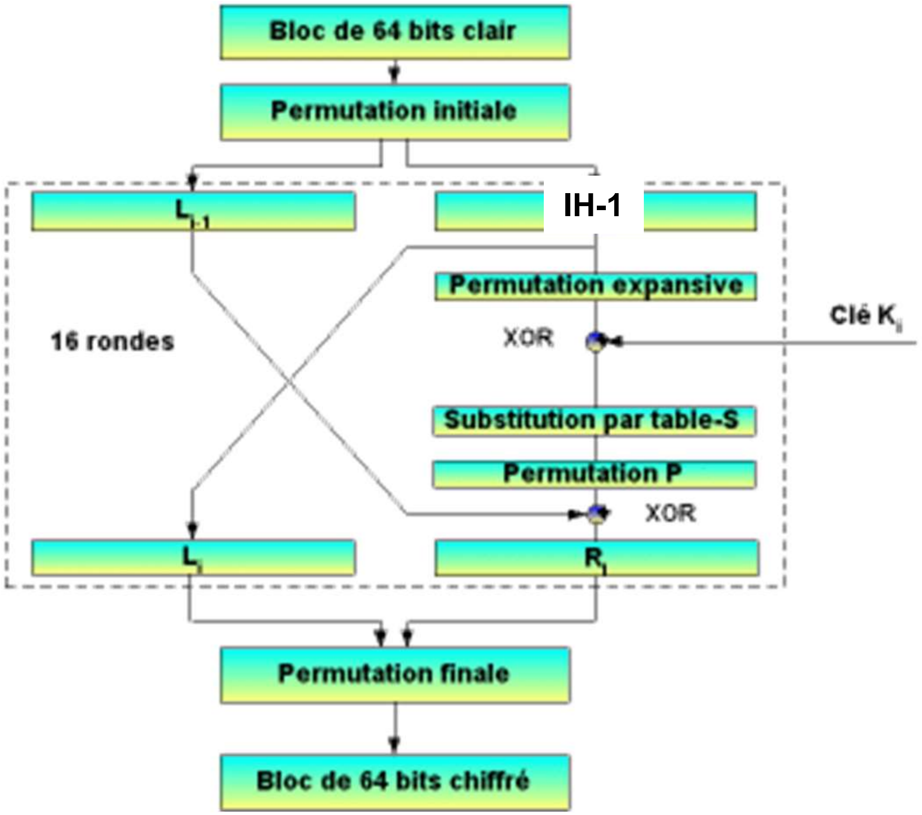
Today software and smart cards industry

Enciphering and deciphering speed (rapidity)

- Can be developed in less than 200 lines
- Very fast on dedicated electronic charts
  - Smart cards
  - Electronic systems of telecommunications

Implementation on Unix, Windows and MacOs available on Internet (chalmers.se/pub for example)

Symmetric cryptography: The standard algorithm for enciphering: IBM DES (Data Encryption Standard)



- Based on XOR functions
- Sequential logics
- Sure
- Rapid
- Easy to implement

but

- Need to exchange the key
  - Problem of security during the transmission of the key

Symmetric cryptography: Flow encryption vs. Block encryption *(chiffrement par flot, par bloc)*

- DES and classical symmetric algorithms are based on block encryption, which means that the message/file to encrypt is divided into blocks
- For some applications, it is interesting to encrypt the message/file at once. Encryption may be achieved without waiting for other data.
- This technics is used for devices with electric consumption constraints (ex: smart phones)
- Based on linear feedback shift register (registre à décalage à rétroaction linéaire)

Symmetric cryptography: Symmetric algorithms

3DES (triple DES)

- It consists in using three times the DES algorithm with three keys k_1, k_2 et k_3 : $m' = DES_{k1}(DES_{k2}(DES_{k3}(m)))$

- Alternative with 2 keys and by using twice the algo of encrypting and once the algo of decoding: $m' = DES_{k1}(DES^{-1}_{k2}(DES_{k1}(m)))$, this alternative is considered more secure

- Another alternative: program TRAN (ripem.msu.edu/pub/crypt/other/tran.shar)

- DESX (DES XORed), GDES (Generalized DES), RDES (Randomized DES)

AES (Advanced Encryption Standard)

- Developed to replace DES and offer a better security

- N.B. At the end of 2003, the American department of defense approved its authorization

- Used in IPSec (secured IP) and IKE (Internet Key Exchange)

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110bb6.html

Conclusion on symmetric systems

- Sure
- Fast

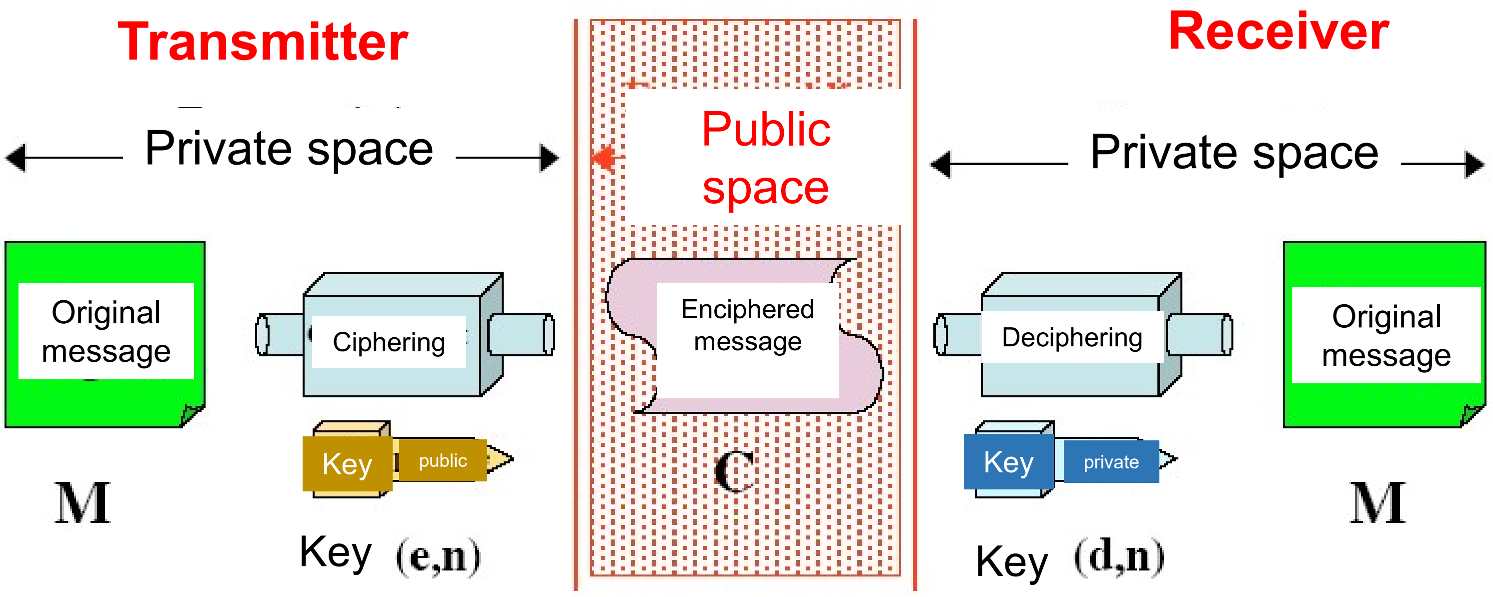
but

- Need to exchange the key
  - Problem of security during the transmission of the key

- Problems of the management of keys

asymmetric Cryptography (couples of private and public key)

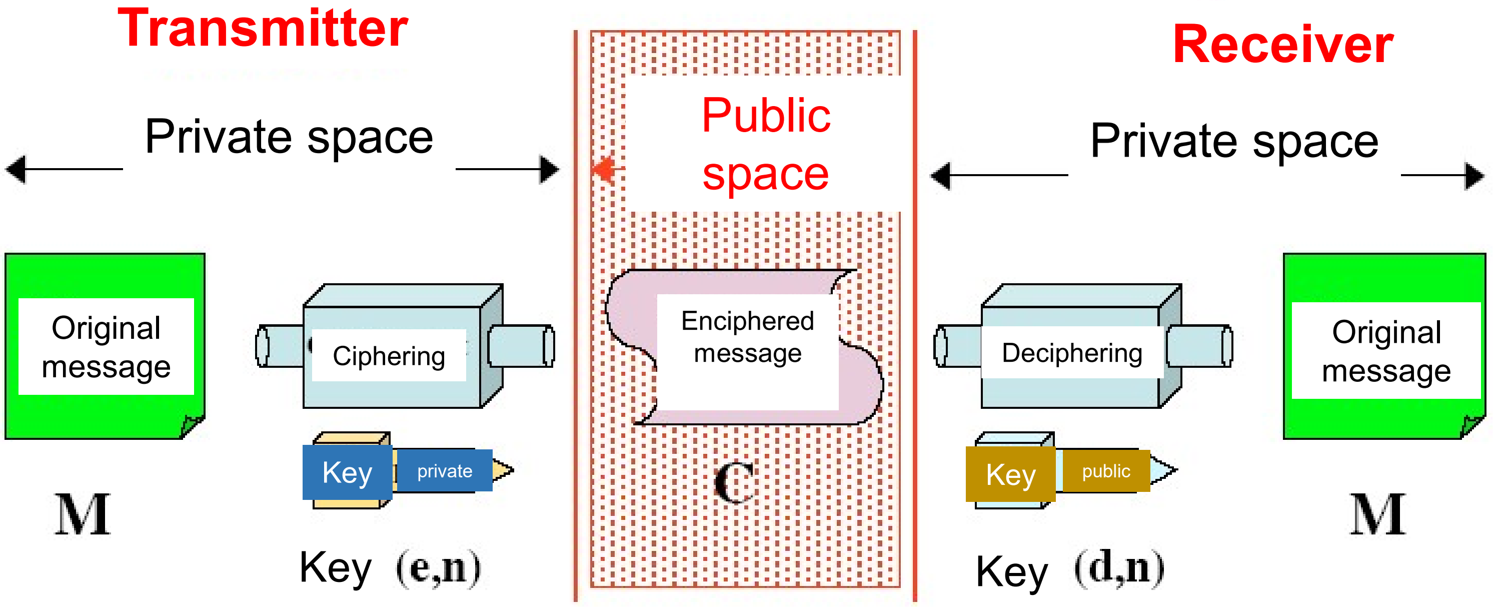
Protection of **confidentiality** = private key on the **receiver** side)



- ✓ Encryption is achieved thanks to the **public** key
- ✓ Warrant that the owner of the private key ONLY can **decrypt** the message

asymmetric Cryptography (couples of private and public key)

Protection of **authentication (signature)** = private key on the **transmitter** side)



- ✓ Encryption is achieved thanks to the **private** key
- ✓ Warrant that the owner of the private key ONLY can **sign** the message

asymmetric Cryptography: RSA ciphering Protocol

Proposed in 1977 by the cryptologists Rivest, Shamir and Adleman

Based on the modular exponentiation (trap function)

Main applications

- Sending of confidential messages to a person
- Authentication by any person of the message sent by an individual
- Authentication by password (smart cards, bank cards)

Security based on the impossibility of carrying out the factorization of a large number of a few hundreds of digits in a reasonable time

- The user selects two large prime numbers p and q, then multiplies them to obtain n=p.q (integer modulating the RSA protocol)

asymmetric Cryptography: RSA

The algorithm is remarkable by its simplicity. It is based on the prime numbers.

To encipher a message:

c = m^e mod n

To decipher: **m = c^d mod n**

- **m** = clear message
- **c** = encrypted message
- **(e, n)** constitutes the public key
- **(d, n)** constitutes the private key
- **n** is the result of the multiplication of 2 prime numbers
- **^** is the power function (a^b: a power b)
- **mod** is the operation of modulo (remainder of the *integer division*)

asymmetric Cryptography: RSA

Creation of a pair of keys

It is simple, but the **e**, **d** and **n** should be chosen with care! And the calculation of these three numbers is delicate.

Methodology:

- The user selects two large prime numbers p and q, and multiplies them to obtain n=p.q (integer modulating the RSA protocol), We should choose p and q with equivalent sizes.

It is advised that n is higher or equal to 512 bits

- Take a number **e** which does not have any factor in common with

(p-1) (q-1).

- Calculate **d** such as **ed mod (p-1)(q-1) = 1**

The couple **(e, n)** constitutes the public key.

(d, n) is the private key.

Various other rules are to be respected for the use of these prime numbers so that the algorithm cannot be "broken"

Prime numbers

- **Largest Known Prime Number:**
- **$2^{82\ 589\ 933}-1$**
- **Found in December 2018, composed of** 24 862 048 digits
- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223…

asymmetric Cryptography: RSA

https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html

Let's encipher the message "**HELLO**". Let's take first the ASCII code (into decimal) of each character and one puts them end to end:

m = 72-69-76-76-79

Then, it is necessary to cut out the message in blocks which is composed of less digits than **n**. **n** is composed of 4 digits, one thus will cut out our message in blocks of 3 digits:

726 976 767 900
(let's complete with zeros)

Then one encrypt each one of these blocks:

726^13 mod **21209** = 11600
976^13 mod **21209** = 5705
767^13 mod **21209** = 16590
900^13 mod **21209** = 3565

The encrypted message is **11600.5705.16590.3565**. One can decipher it with d:

11600^1609 mod **21209** = 726
5705^1609 mod **21209** = 976
16590^1609 mod **21209** = 767
3565^1609 mod **21209** = 900

I.e. the digit suite: **726976767900**.
We find the clear message: **72 69 76 76 79**: "**HELLO**".

symmetric vs. asymmetric Cryptography

- Asymmetric ciphering more useful
  - No problem with the key transfer
  - Allow the message signature
  - Possibility to manage Public Key Infrastructure (PKI)
- Symmetric encryption is faster (La Recherche, June 2018)
  - AES allows enciphering many gigabytes per second on a recent processor
  - Asymmetric cryptography standards reach less than one megabyte per second (1000 to 10000 slower !)
- Generally the two strategies are combined
  - Interest: to use a protocol with public key to transmit the DES key => hybrid cryptography

Hybrid cryptography: generation of a sharing key

Two users will design a common key which will be useful for them only

ASYMMETRIC ASPECT

They choose n the multiple of 2 prime numbers p and q and an integer a (a and n can be known (not confidential))

Then each one chooses an integer X belonging to [1, n-1] and calculates the integer $Y=a^{X}$ mod n

We obtain two couples (X_1,Y_1) and (X_2, Y_2) where the values Y_1 and Y_2 will be published

HYBRID ASPECT

Each one of them can then calculate the key $c=a^{X1X2}$ mod n because $c=(Y1^{X2}$ mod n$)=(Y2^{X1}$ mod n)

R: Each one knows its own X only

Security comes from the fact that it is impossible in a reasonable time to obtain the key C by the calculation of a discrete logarithm (unfeasible in a reasonable time taking into account the size of p and q)

SYMMETRIC ASPECT

Users can now exchange encrypted data using a symmetric system with the common key c

Application

- User 1

- User 2

n

a

Application

- User 1
- X1 : private key

n

a

- User 2
- X2 : private key

Application

- User 1
- X1 : private key
- $Y1=a^{X1}$ mod n : public key

n

a

- User 2
- X2 : private key
- $Y2=a^{X2}$ mod n : public key

Application

- User 1
- X1 : private key
- $Y1=a^{X1}$ mod n : public key
- Send Y1 to user 2
- Receive Y2

n

a

- User 2
- X2 : private key
- $Y2=a^{X2}$ mod n : public key
- Send Y2 to user 1
- Receive Y1

Application

- User 1
- X1 : private key
- $Y1=a^{X1}$ mod n : public key
- Send Y1 to user 2
- Receive Y2
- $c=(Y2^{X1} \bmod n)$

n

a

- User 2
- X2 : private key
- $Y2=a^{X2}$ mod n : public key
- Send Y2 to user 1
- Receive Y1
- $c=(Y1^{X2} \bmod n)$

Application

- User 1
- X1 : private key
- $Y1=a^{X1}$ mod n : public key
- Send Y1 to user 2
- Receive Y2
- $c=(Y2^{X1}$ mod n)
- Key « c » in order to use the symmetric system

n

a

- User 2
- X2 : private key
- $Y2=a^{X2}$ mod n : public key
- Send Y2 to user 1
- Receive Y1
- $c=(Y1^{X2}$ mod n)
- Key « c » » in order to use the symmetric system

Private and public keys

- The public key is composed of two large prime numbers p and q (several hundreds of bits).
- The public key contains n =p*q.
- As n est very large, it is impossible to find all the possible factorisations.
- The knowledge of n does not allow to deduce the values of p and q.

Hybrid cryptography: generation of a sharing key: exercise

Generate a shared key with your neighbor

(ex:

- a=3 et n=14 (public values (known)) n=2*7
- X_1 = 4 (secret value known only by the participant on the left)
- X_2 = 3 (secret value known only by the participant on the right)

Exercise

- Generate a sharing key with your neighbor
- (ex:
  - a=3 et n=14 (public values (known)) n=2*7
  - X_1 = 4 (secret value known only by the participant on the left)
  - X_2 = 3 (secret value known only by the participant on the right)

  - Y1=a^{X1} mod n = 3^4 mod 14 = 11
  - Y2=a^{X2} mod n = 3^3 mod 14 = 13
  - c=$Y2^{X1}$ mod n =
  - c=$Y1^{X2}$ mod n =

Exercise

- Generate a sharing key with your neighbor
- (ex:
  - a=3 et n=14 (public values (known)) n=2*7
  - X_1 = 4 (secret value known only by the participant on the left)
  - X_2 = 3 (secret value known only by the participant on the right)

  - $Y1=a^{X1}$ mod n = 3^4 mod 14 = 11
  - $Y2=a^{X2}$ mod n = 3^3 mod 14 = 13
  - $c=Y2^{X1}$ mod n = 13^4 mod 14 = 1
  - $c=Y1^{X2}$ mod n = 11^3 mod 14 = 1

Cryptography: Some considerations on breaking a 768-bit RSA key

- From an Inria document, 2010.

- Key used for bank cards

- To break the key, find the prime numbers which compose the key: it is a number composed of 232 figures (2^{768})…

- Need efficient algorithm

- Need large calculation capacities: use of Grid’5000 => 1544 computers with more than 5000 cores.

- Collaboration with CH, JP, NL, DE : on average 1700 cores used during one year of calculation…

- One week by using the supercomputer *Jaguar* (from *Oak Ridge National Laboratory*) if available (not such computers in Europe…)

- The purpose was to show if it is possible to break using grid of « classical » computers

- Next step: to break a 1024 bit-key => it should be possible around 2020

- Advise from ANSSI (2010):

  Use at least 1536 bit-keys for applications until 2010

  Use at least 2048 bit-keys for application beyond 2010

Exercise

1. A group of N people wishes to use a cryptographic system to exchange confidential information by pair of people. The information exchanged between two members of the group will not have to be able to be read by any other member. The group decides to use a symmetric ciphering system.
2. Which is the minimal number of symmetric keys necessary?
3. Give the name of a known symmetric encryption algorithm.
4. The group then decides to replace this system by an asymmetric system.
5. Which is the minimal number of couples of asymmetric keys necessary so that each member can send and receive encrypted and/or signed information? If it is considered that each one can communicate with everyone, how many private and public keys each user will have it to hold (keep)?
6. The group finally decides to use a Public Key Infrastructure (PKI, certificates).
7. What is the interest to use such a system?
8. How many keys each user should finally managed? How many keys are there globally?
9. Bob wishes to send encrypted and signed information to Alice (Bob and Alice belong both to the group). Which key(s) Bob should use?
10. Give the name of a known asymmetric encryption algorithm.
11. The group finally decides to use a hybrid system for the ciphering (i.e. which uses symmetric and asymmetric cryptography).
12. Give the reasons why such a system can be efficient.

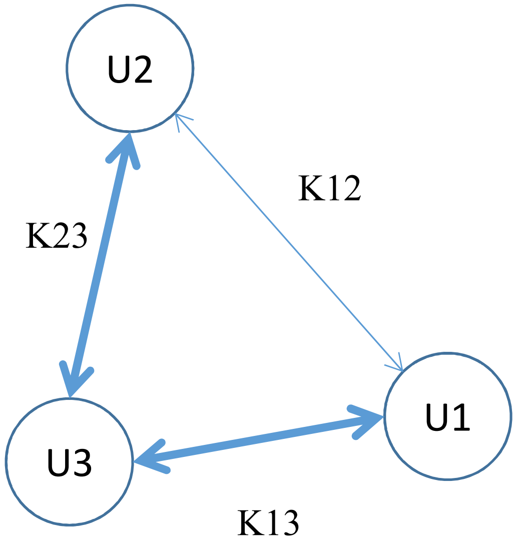
Ex

- 2. N people

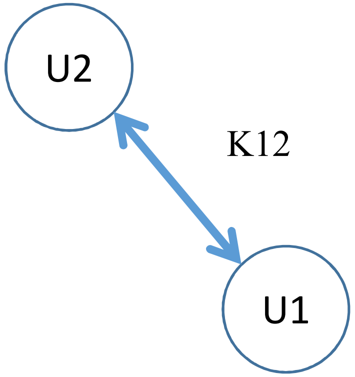
$$C_n^2 = \frac{N!}{2!.(N-2)!} = \frac{N.(N-1)}{2}$$ is the number of symmetric keys needed

- 3. DES, AES, 3DES…
- 5. N pairs of keys is the number of asymmetric keys needed (or 2.N keys)
- 7. PKI
- 8. N+1 keys are possible for one computer (my private key + my public key (to send to others not to use myself) + N-1 public keys from the other users)
- 9. To encrypt, Bob needs the public key of Alice, then to sign, Bob needs his own private key.
  - (beyond the exercise) : After reception, Alice will first verifying the signature using the public key of Bob, then Alice will decrypt using her own private key.
  - (beyond the exercise) : it is considered that the needed public keys have been exchanged before the transaction
- 10. RSA
- 12. It is more efficient to manage an asymmetric system (using a PKI) in which we manage actually 2.N keys (N pairs of keys) than to manage a symmetric system with N.(N-1)/2 keys

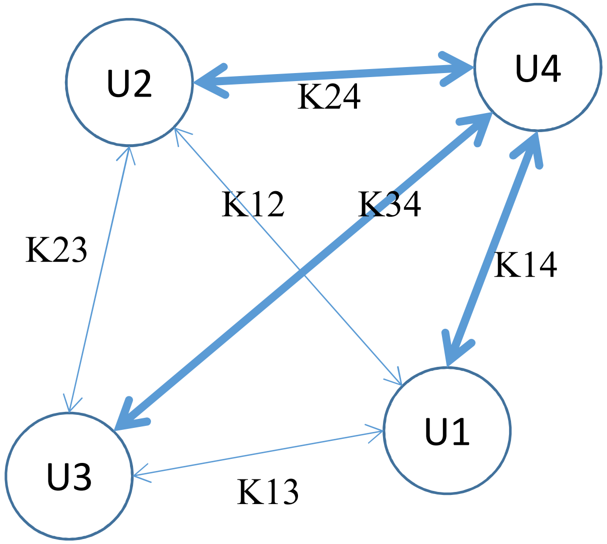
3 users, 3 keys



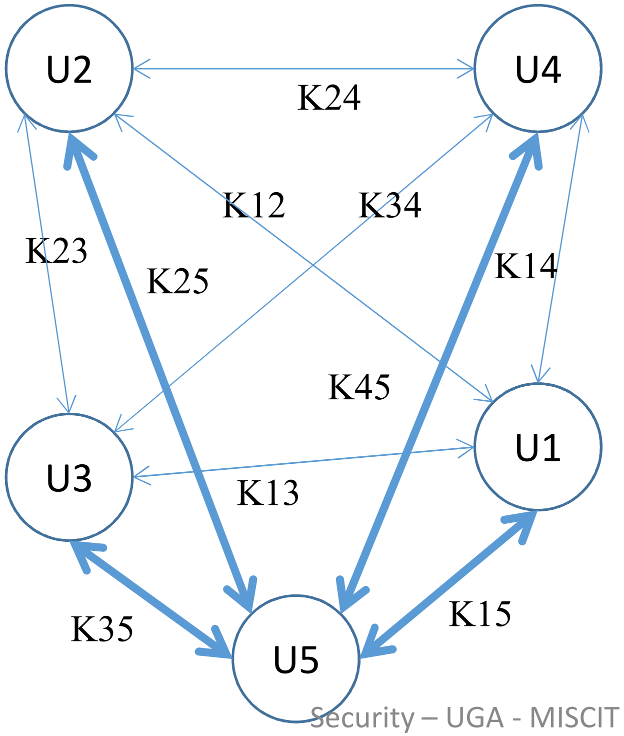
2 users, 1 key



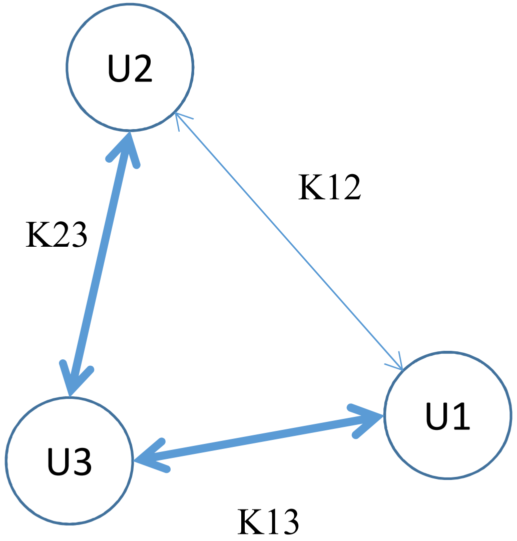
4 users, 6 keys



5 users, 10 keys

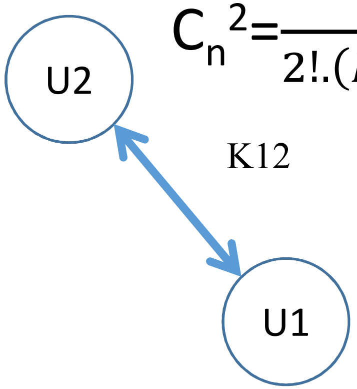


3 users, 3 keys

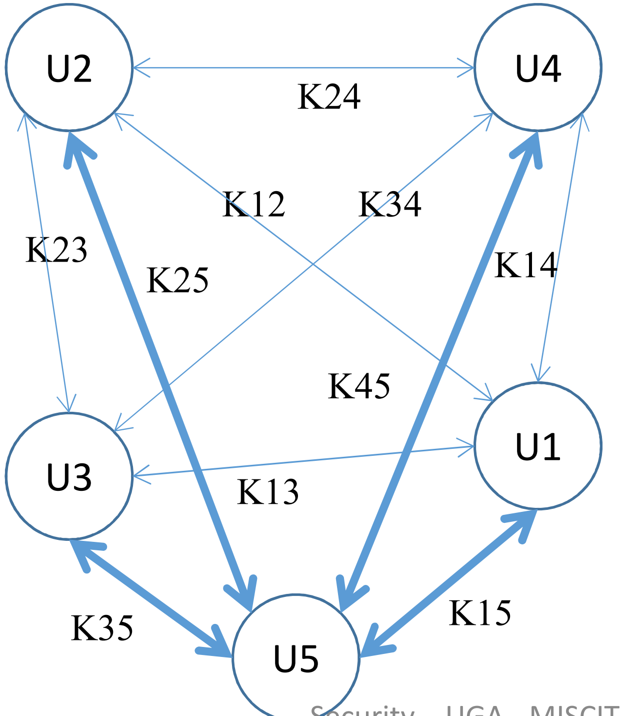


2 users, 1 key

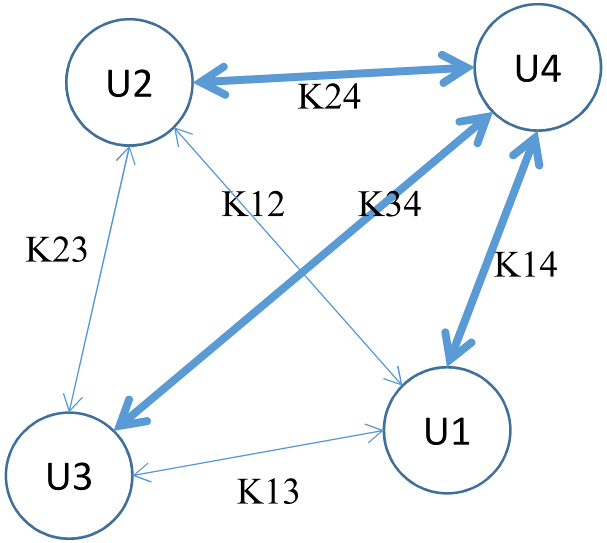
$$C_n{}^2 = \frac{N!}{2!.(N-2)!} = \frac{N.(N-1)}{2}$$



5 users, 10 keys



4 users, 6 keys



Conclusions on cryptography

- Hybrid cryptography

- Difficult implementation of asymmetric cryptography

- Integrated in the certificates

- Integrated in security protocols (IPSec, SSL/TLS)

- Integration of cryptography and more generally of security mechanisms in industrial applications

6.5 Intrusion detection and response

- Purpose: to detect and respond to network attacks and malicious code (anti-virus)

- Malicious code

  Intended to harm, disrupt, or circumvent computer and network functions (viruses, trojan horses, worms…)

- Network attacks

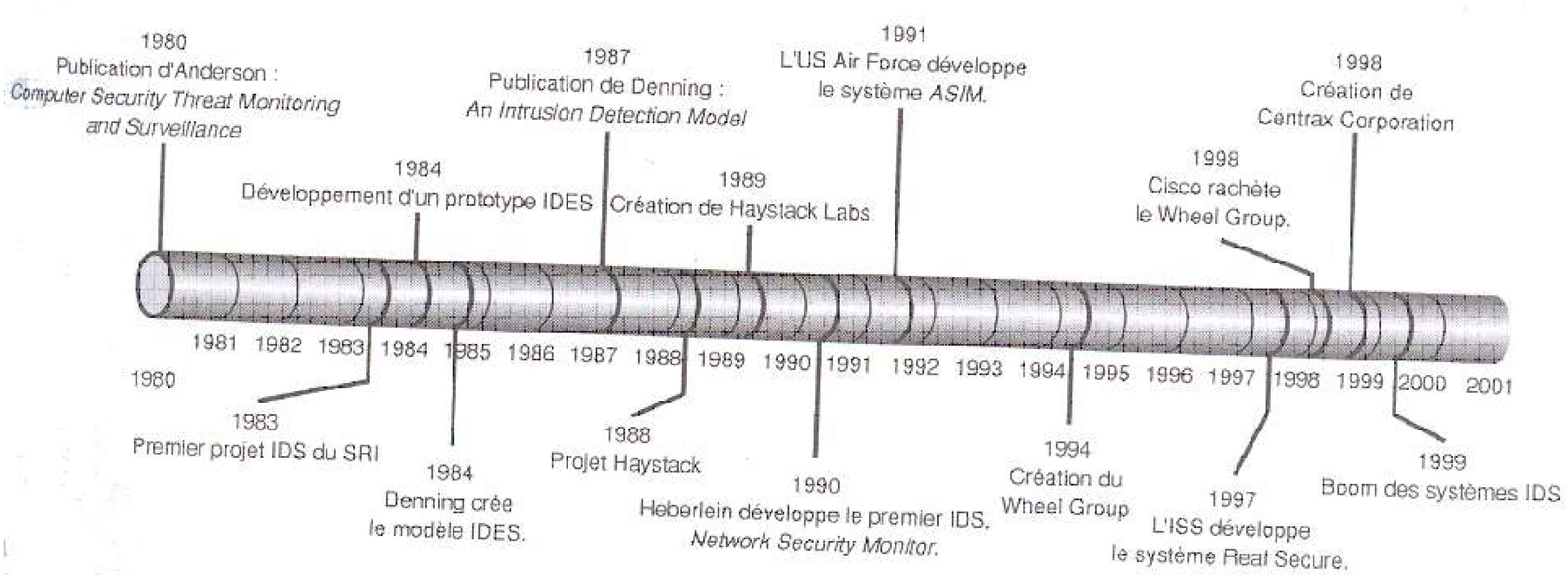
  Modification attacks: unauthorized alteration of information

  Repudiation attack: denial that an event or transaction ever occurred

  Denial-of-service attack: actions resulting in the unavailability of network resources and services, when required

  Access attacks: unauthorized access to network resources and information

History of the development of IDS (for IT)


1980
Publication d'Anderson :
Computer Security Threat Monitoring and Surveillance
1987
Publication de Denning :
An Intrusion Detection Model
1991
L'US Air Force développe le système *ASIM*.
1998
Création de Centrax Corporation
1984
Développement d'un prototype IDES
1989
Création de Haystack Labs
1998
Cisco rachète le Wheel Group.
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
1983
Premier projet IDS du SRI
1984
Denning crée le modèle IDES.
1988
Projet Haystack
1990
Heberlein développe le premier IDS.
Network Security Monitor.
1994
Création du Wheel Group
1997
L'ISS développe le système Real Secure.
1999
Boom des systèmes IDS

Today, the products implement concepts dating from the years 1980

Signature-based IDSs

Signature-based IDSs: signature or attributes that characterizes an attack are stored for reference (if there is a match, a response is initiated)

Advantages

- Low false alarm rates
- Standardized (generally)
- Understandable by security personnel

Disadvantages

- Failure to characterize slow attacks that extend over a long period of time
- Only attack signatures that are stored in the database are detected
- Knowledge database needs to be maintained and updated regularly
- Because knowledge about attacks is very focused (dependent on the operating system, version, platform, and application), new, unique, or original attacks often go unnoticed

Statistical anomaly-based IDSs

Statistical anomaly-based or behavior-based IDSs: dynamically detects deviations from the learned patterns of « normal » user behaviour and trigger an alarm when an intrusive activity occurs

Needs to learn the « normal » usage profile (which is difficult to determine)

Advantages

- Can dynamically adapt to new, unique, or original vulnerabilities
- Not as dependent upon specific operating systems as a knowledge-based IDS

Disadvantages

- Does not detect an attack that does not significantly change the system-operating characteristics
- High false alarm rates. High positive are the most common failure of behavior-based ID systems
- The network may experienced an attack at the same time the intrusion detection system is learning the behaviour

Functionalities of IDS:
Responses to the detected intrusions

Active answers

- -To undertake an aggressive action against the intruder
  - (! Attention with legality!)
- -To restructure the network architecture
  - To isolate the attacked system
  - To modify the environment parameters which made the intrusion possible
- -To supervise the attacked system
  - To collect information in order to understand the intrusion
  - To identify the author of the intrusion and his approach
  - To identify security failures

Passive answers

- -Generation of an alarm
- -Emission of a SMS message towards the administrator

Some tools (for IT)

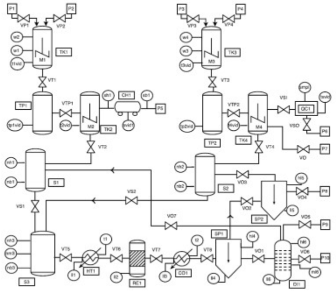
- -Snort, Suricata, Bro, Cisco secure IDS, Billy Goat, Enterasys

7. Industrial control Systems [Stouffer 2011]

Generic term regrouping

SCADA (Supervisory Control And Data Acquisition)

- Distributed on several geographical areas



DCS (Distributed Control Systems)

- Just in a local zone

other configurations based on **PLC** (Process Logic Controller)

Evolution of ICS systems

- Previously isolated and using proprietary protocols

- Security not taken into account (security by obscurity)

- Now more and more connected for economic reasons

- Use of classical IT solutions (architecture, OS, network protocols)

- More vulnerable to attacks

Comparison between ICS and classical IT systems

Category	IT systems	ICS systems
Performances	Delays and jigs acceptable	Real time, critical time Strict time constraints
Availability	Some tolerance on degradations, depending on situations	High availability Inacceptable loss of connection (depends) Advance planning
Resource constraints	Available resources	Design for industrial processes Limited processing and memory resources
Targeted properties	Confidentiality Integrity Availability	Timeliness Availability Integrity Confidentiality

ICS Specificities

	Information Technology	*Operation Technology*
Cyber security culture	Awareness of risks Methods and tools	Recent
Life duration	3-5 years	> 20 years
Performance	Throughput	Latency Real-time constraints
Resources	Abundant	Limited
Networks Protocols topologies	Numerous connection points Dynamic topologies	Fixed topologies “Simple” protocols Defined communication strategy, scheduling
Security Attributes	Cyber sécurity: Confidentiality Integrity Availability	Dependability: Availability Reliability Safety

Some other considerations on ICS

- Define the model of trust
- Define the model of threats
- Vulnerabilities linked to security procedures and policy
- Vulnerabilities linked to the architecture
- Vulnerabilities linked to networks

- Control systems

    Communication: protocole, flow
    Tasks: state, scheduling
    Resources: memory, cpu, traffic
    Data and control flows: timestamp, values intervalles

Conclusions on Cyber-security of CPS

- New issues

- Integration of the IT and ICS worlds (convergence)

- Double culture (computer science/engineering and automation)

- Behaviour of the system

- Security of the Communication/Information system
=> Safety of the networked control system

- Implementation of cryptography

- In-depth security

References

- JF Aubry, N. Brinzei – Systems Dependability Assessment – Wiley, 2015
- M. A. Azgomi & A. Movaghar – Definition and analysis of cloured stochastic activity networks – Technical report, Dept. Of Computer Engineering, Sharif University of Technology, Tehran, Iran, 2004.
- P. Barger – Evaluation et validation de la fiabilité et de la disponibilité des systèmes d'automatisation à intelligence distribuée, en phase dynamique – thèse de l'Université Henri Poincaré Nancy 1, 15 décembre 2003.
- M. Bayart – *Instrumentation intelligents, systèmes automatisés de production à intelligence distribuée* – Habilitation à Diriger des Recherches, USTL, Lille, 21 décembre 1994.
- A. Carneas & al. – Secure control: towards survivable cyber-physical systems – 28th International Conference on Distributed Computing Systems Workhop – 2008.
- A. Cervin, D. Henriksson, B. Lincoln, J. Eker, K.E. Årzén – How does control timing affect performance? – IEEE Control Systems Magazine, JUne 2003, Vol. 23, N.3
- Groupe CIAME – Réseaux de terrain, description et critères de choix – Hermes, Paris, 1999.B. Conrard – Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception – thèse de l'Université Henri Poincaré Nancy 1, 24 septembre 1999.
- Blaise Conrard, Jean-Marc Thiriet, Michel Robert – Problems of precision for control loops implanted on Distributed Automation System – CESA'98 (Computational Engineering in Systems Applications)/IMACS/IEEE, Hammamet/Nabeul (Tunisie), avril 1998, pp. 180-185, vol. 1.
- M. Conti, S. Giordano – Multihop ad hoc networking: the theory – IEEE Communications, Vol 45, n°4, p.78, avril 2007.
- R. David, H. Alla – Discrete, continuous, and hybrid Petri Nets – Springer, 2010 .
- M. Diaz – Les réseaux de Petri, modèles fondamentaux – Hermes, Paris, 2001.
- JP Georges – Systèmes contrôlés en réseau : évaluation de performances d’architectures ethernet commutées – thèse UHP-CRAN, Nancy, 2005.
- F. Hohlbaum, M. Braendle, F. Alvarez – Practical considerations for implementing IEC 62351 – ABB, 2009
- W. Hu, D. Willkomm, G. Vlantis, M. Gerla, A. Wolisz – Dynamic frequency hopping communities for efficient IEEE 802.22 operation – IEEE communications, vol 45, n° 5, mai 2007, p. 80
- K. Jensen – Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use – Monographs in Theoretical Computer Science, Springer-Verlag, 2nd corrected printing 1997.
- Guy Juanole – Réseaux de communication et automatique – *Journées "Automatique et Communication"*, 13-14 mars 2001.
- G. Juanole, I. Blum – Quality of service of real time networks and performances of distributed applications – LAAS report 99166, avril 1999.

References

- F. Jumel, J.M. Thiriet, J.F. Aubry, O. Malasse - "Towards an information-based approach for the dependability evaluation of distributed control systems" - 20th IEEE Instrumentation and Measurement Technology Conference (IEEE/IMTC2003), Vail (Colorado, United States), 20-22nd May 2003, pp. 270-275.
- P. Kleinschmidt, F. Schmidt - How many sensors does a car need ? - Eurosensors V, Roma, 2 October 1991, pp.1-13.
- P.R. Kumar – New technological vistas for systels and control – IEEE Control Magazine, February 2001
- M.J. Lee, J. Zhang & al. – A new taxonomy of routing algorithms for wireless mobile ad hoc networks: the component approach – IEEE p. Communications, Vol. 44, N° 11, novembre 2006, 116
- K. Lu, Y. Qian – A secure and service-oriented network control framework for WIMAX network – IEEE Communications, Vol 45, N° 5, p. 124, mai 2007
- Stéphane Mocanu – Cours de réseaux, ENSIEG, 2005
- R. M. Murray, K.J. Åström, S. P. Boyd, R. W. Brockett, G. Stein – Future directions in control in an information-rich world, IEEE Control Magazine, April 2003, Vol. 23, n. 2
- Natale, O.R.; Sename, O.; Canudas-de-Wit, C.; - Inverted pendulum stabilization through the Ethernet network, performance analysis - American Control Conference, 2004. Proceedings of the 2004 - Volume 6, 30 June-2 July 2004 Page(s):4909 - 4914 vol.6
- Q. Ni, A. Vinel, Y. Xiao, A. Turlikov, T. Jiang – Investigation of bandwidth request mechanisms under point-to-multipoint mode of Wimax networks – IEEE Communications, Vol 45, N° 5, p. 132, mai 2007
- S.I. Niculescu – Systèmes à retard, aspects qualitatifs sur la stabilité et la stabilisation – Diderot éditeur, Paris, 1997.
- D. Niyato, E. Hossain – Integration of WImax and Wifi: optimal pricing for nadwidth sharing – IEEE Communications, Vol 45, N° 5, p. 140, mai 2007.
- L. Ondrej, M. Mlanic, T. Vollmer – Improving cyber-security of amrt grids systems via anomay detection and linguistic domain knowledge – 2012.
- L. Pelusi, A. Passarella, M. Conti – Opportunistic networking: data forwarding in disconnected mobile ad hoc network, IEEE Communications, Vol. 44, N° 11, novembre 2006.
- S.A. Reinemo, T. Skeie, T. Sodring, O. Lysne, O. Torudbakken – An overview of QoS capabilities in InfiniBand, Advanced Switching Interconnect, and Ethernet – IEEECommunications, Vol 44, n° 7, juillet 2006, page 32
- M. Robert, M. Marchandiaux, M. Porte – *Capteurs Intelligents et Méthodologie d'Evaluation* – Hermès, 1993.
- D. J. Smith & K. G. Simpson – Functional safety (second edition) a straightforward guide to applying IEC 61508 and related standards – Elsevier, 2004.
- Y. Q. Song – performance analysis and improvement of zig-bee routing protocol – Fet, 2007, Toulouse.
- Stouffer, K. A., Falco, J. A., and Scarfone, K. A. (2011). Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc). Technical report, Gaithersburg, MD, United States.

References

- J.M. Thiriet - Habilitation à Diriger des Recherches de l'Université Henri Poincaré Nancy 1 en Automatique : "Sûreté de fonctionnement de Systèmes d'Automatisation à Intelligence Distribuée" - CRAN-UHP, Nancy, 16 décembre 2004.
- Törngren M. – Fundamentals of implementing real-time control applications in distributed computer systems, Real-Time Systems Journal, Volume 14, Number 3, May 1998.
- V. Volovoi – Modeling multiphased missions using stochastic Petri nets with aging tokens – RAMS'04, Annual Reliability and Maintainability Symposium, Los Angeles, janvier 2004.
- G.C. Walsh, H. Ye – Scheduling of networked control systems – IEEE control Magazine, février 2001.
- Witrant, E.; Canudas-De-Wit, C.; Georges, D.; Alamir, M.; - Remote stabilization via time-varying communication network delays: application to TCP networks - Control Applications, 2004. Proceedings of the 2004 IEEE International Conference on - Volume 1, 2-4 Sept. 2004 Page(s):474 - 479 Vol.1
- J. Zaytoon – Systèmes dynamiques hybrides – traité ic2 série systèmes automatisés, Hermes, 2002.
- W. Zhang, M.S. Branicky, S.M. Philips – Stability of networked control systems – IEEE control Magazine, février 2001.
- Zhou, C., Huang, S., Xiong, N., Yang, S.-h., Li, H., Qin, Y., and Li, X. (2015). Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 45(10):1345–1360
- J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- S. Ghernaouti-Hélié – *Sécurité informatique et réseaux* – Dunod, 2005.
- C. Davis, M. Schiller, K. Wheeler - *IT Auditing: using control to protect assets* – 2007, Mc Graw Hill
- D. Vergnaud – *Exercices et problèmes de cryptographie* – 2ème édition, 2015, Dunod

References

[1] Andrew J. Kerns, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. 2014. Unmanned Aircraft Capture and Control Via GPS Spoofing. J. Field Robot. 31, 4 (July 2014), 617-636
[2] L. He, W. Li, C. Guo and R. Niu, "Civilian Unmanned Aerial Vehicle Vulnerability to GPS Spoofing Attacks," *2014 Seventh International Symposium on Computational Intelligence and Design*, Hangzhou, 2014, pp. 212-215
[3] Z. Feng *et al*., "Efficient drone hijacking detection using onboard motion sensors," *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, Lausanne, 2017, pp. 1414-1419.
[4] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. Rocking drones with intentional sound noise on gyroscopic sensors. In Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15)
[5] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling uavs with sensor input spoofing attacks," in 10th USENIX Workshop on Offensive Technologies (WOOT 16), (Austin, TX), USENIX Association,2016.
[6] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya và S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," trong *Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International*, Paphos, Cyprus, 2016
[7] Guillaume Fournier, Paul Audren de Kerdrel, Pascal Cotret, Valérie Viet Triem Tong. DroneJack: Kiss your drones goodbye!. SSTIC 2017 - Symposium sur la sécurité des technologies de l'information et des communications, Jun 2017, Rennes, France. pp.1-8. 〈hal-01635125〉
[8] M. Heiges, R. Bever and K. Carnahan, "How to Safely Flight Test a UAV Subject to Cyber-Attacks," Systems Engineering Research Center, 2014.
[10] A. Y. Javaid, W. Sun, V. K. Devabhaktuni và M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," trong Homeland Security (HST), 2012 IEEE Conference on Technologies for, Waltham, MA, USA, 2013
[11] "ISO/IEC 27005:2011 Information technology - Security technique - information security[managment," ISO/IEC, 2011.
[12] "MEHARI-Overview," Clusif, Paris, 2010.
[13] AIRWORTHINESS SECURITY PROCESS SPECIFICATION ED-202 / DO-326. [Performance]. EUROCARE/RTCA, 2014.
[14] EVITA, "D2.3 Security requirements for automotive on-board networks based on dark-side scenarios," EVITA, 2009
[15] JARUS guidelines on Specific Operations Risk Assessment (SORA), 2017
[16] Livre "System engineering fundamental", Defense Acquisition University, Virginal, 2011
[17]B. Schneier, "Modeling security threats," Dr. Dobb's Journal, 12 1999.
[18] Eric J. Byres, Matthew Franz , Darrin Miller, "The use of attack trees in assessing vulnerabilities in SCADA systems," in IEEE Conf. International Infrastructure Survivability Workshop, 2004.
[19] S. Gil-Casals, Thèse "Risk assessment and Intrusion detection for airbone networks," Hal, Toulouse, 2014.
[20] Dr. Barry Horowitz et al, "System Aware Cyber Security for an Autonomous Surveillance System On Board an Unmanned Arial Vehicle"
[21] Silvia Gil-Casals. Risk Assesment and Intrusion Detection for Airborne Networks. Networking and Internet Architecture [cs.NI]. INSA
[22]T J. Xu, K. K. Venkatasubramanian and V. Sfyrla, "A methodology for systematic attack trees generation for interoperable medical devices," 2016 Annual IEEE Systems Conference (SysCon), Orlando, FL, 2016, oulouse, 2014. English

References

- “Stuxnet”, in L’Informaticien, Nov. 2010.
- L. Bloch, C. Wolfhugel, A. Kokos, G. Billois, A. Soullié, A. Anzala-Yamakajo, T. Debize, Sécurité informatique, pour les DSI, RSSI et administrateurs, 5ème edition, Eyrolles, 2016.
- M. Cislo, Virus and industrial processes, WINS/CNMS Bachelor memoir, Univ. Grenoble Alpes, Grenoble, 2015.
- N Falliere, L. O. Murchu, and E. Chien. W32.stuxnet dossier. https://www.symantec.com/content/en/us/enterprise/media/security_response/ whitepapers/w32_stuxnet_dossier.pdf, 2011. [Online, acc. : March-2018].
- US-CERT. Crashoverride. https://www.us-cert.gov/ncas/alerts/TA17-163A, 2017. [Online, acc. : March-2018]
- Dragos. Crashoverride: Analysis of the threat to electric grid operations. lhttps://dragos.com/blog/crashoverride/, 2017. [Online, acc. : July-2018]
- O. Koucham, Détection d’intrusions pour les systèmes de contrôle industriels, thèse de Doctorat, Univ. Grenoble Alpes, 2018.
- A. Mkhida, Contribution à l’évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l’Intelligence, thèse de Doctorat, Univ. de Lorraine, 2008.
- J. C. Laprie, Sûreté de fonctionnement et tolérance aux fautes : concepts de base, rapport LAAS n°88.287, paru dans les techniques de l’ingénieur, 1988.
- R. Ghostine, Influence des fautes transitoires sur la fiabilité d’un système commandé en réseau, thèse de Doctorat, Univ. de Lorraine, 2008.
- CEI 61508. Sécurité fonctionnelle des systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité. Commission Electrotechnique Internationale, Genève, Suisse, 2000.
- G. Moncelet. Application des réseaux de Petri à l’évaluation de la sûreté de fonctionnement des systèmes mécatroniques du monde automobile, Thèse de Doctorat, N°3076, Université Paul Sabatier, Toulouse, 9 octobre (1998).
- P.J. Portugal, and A. Carvalho. A Stochastic Petri Net Framework for Dependability Evaluation of Fieldbus Networks – A Controller Area Network (CAN) Example. International IEEE Conference in Mechatronics and Robotics, MECROB, 2004.
- Navet, N., Y. Song and F. Simonot. Worst-Case Deadline Probability in Real-Time Applications Distributed over Controller Area Network. In: Journal of systems Architecture. Vol (46), No. 1, p: 607-617, 2000.
- J. Galdun, JM Thiriet, J. Liguš, Study of different load dependencies among shared redundant systems, International Workshop on Real Time Software RTS'2008 within International Multiconference on Computer Science and Information Technology IMCSIT'2008, October 20–22, Wisla, Poland, pp. 609 – 615, ISSN 1896-7094, 2008.
- R. Ghostine, JM Thiriet JF Aubry, M. Robert, A Framework for the Reliability Evaluation of Networked Control Systems, 17th IFAC World Congress, July 6-11, pp. 6833-6838, 2008.
- P. Barger, JM Thiriet, M. Robert, Dependablity study in distributed control systems integrating smart devices, Low Cost 2004, Ottawa (Canada), pp. 79-84, 2004.
- J. Tixier, G. Dusserre, O. Salvi, D. Gaston, ‘Review of 62 risk analysis methodologies of industrial plants’, Journal of Loss Prevention in the process industries 15, pp. 291–303. 2002.
- C. Davis, M. Schiller, K. Wheeler, IT Auditing: using control to protect assets, Mc Graw Hill, 2007.
- E. Cole, R. Krutz, JW Conley, Network security bible, Wiley, 2005.
- D. Diallo, M. Feuillet, Détection d’intrusion dans les systèmes industriels : Suricata et le cas de Modbus, CAESAR 2014, website of ANSSI, [Online, acc. : October-2018].
- S. Cheung and K. Skinner. Using Model-based Intrusion Detection for SCADA Networks. In Proc. SCADA Security Scientific Symposium, pages 127–134, 2007.
- H. Lin, A. Slagell, C. Di Martino, et al. Adapting Bro into SCADA: building a specification-based intrusion detection system for the DNP3 protocol. In Proc. CSIIRW ’13, pages 1–4, 2013.

References

- N. Goldenberg and A. Wool. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. International Journal of Critical Infrastructure Protection, 6(2):63–75, 2013.
- A. Kleinmann and A. Wool. Accurate modeling of the siemens s7 scada protocol for intrusion detection and digital forensics. Journal of Digital Forensics, Security and Law, 9(2), 2014.
- R. Barbosa, R. Sadre, and A. Pras. Flow whitelisting in SCADA networks. Int. Journal of Critical Infrastructure Protection, 6(3-4):150–158, December 2013.
- H. Hadeli, R. Schierholz, M. Braendle, and C. Tuduce. Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration. In IEEE Conference on Emerging Technologies and Factory Automation ETFA 2009, pages 1–8, 2009.
- S. Ponomarev and T. Atkison. Industrial Control System Network Intrusion Detection by Telemetry Analysis. IEEE Transactions on Dependable and Secure Computing, 5971(c):1–1, 2015.
- D. Yang, A. Usynin, and J. Hines. Anomaly-based intrusion detection for SCADA systems. In 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC&HMIT 05), pages 12–16, 2005.
- R. Ramos, R. Barbosa, R. Sadre, and A. Pras. Difficulties in Modeling SCADA Traffic : A Comparative Analysis. In Proceedings of the 13th international conference on Passive and Active Measurement (PAM ’12), pages 126–135, 2012.
- O. Linda, T. Vollmer, and M. Manic. Neural Network based Intrusion Detection System for critical infrastructures. 2009 International Joint Conference on Neural Networks, pages 1827–1834, 2009.
- C. Zimmer, B. Bhat, et al. Time-based intrusion detection in cyber-physical systems. In Proc. First ACM/IEEE Int. Conf. on CPS, pages 109–118, 2010.
- J. Rrushi and K.-D. Kang. Detecting Anomalies in Process Control Networks. IFIP Advances in Information and Communication Technology, 311:151–165, 2009.
- J. Reeves, A. Ramaswamy, M. Locasto, S. Bratus, and S. Smith. Intrusion detection for resource-constrained embedded control systems in the power grid. International Journal of Critical Infrastructure Protection, 5(2):74–83, 2012.
- C. Bellettini and J. L. Rrushi. A product machine model for anomaly detection of interposition attacks on cyber-physical systems. IFIP International Federation for Information Processing, 278:285–299, 2008.
- D. Hadziosmanovic, R. Sommer, and E. Zambon. Through the Eye of the PLC: Towards Semantic Security Monitoring for Industrial Control Systems. In Proc. ACSAC 14, 2014.
- N. Erez and A. Wool. Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems. International Journal of Critical Infrastructure Protection, 10:59–70, 2015.
- A. Carcano, I.N. Fovino, M. Masera, and A. Trombetta. Statebased network intrusion detection systems for SCADA protocols: A proof of concept. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6027 LNCS:138–150, 2010.
- I. N. Fovino, A. Carcano, T. D. L. Murel, A. Trombetta, and M. Masera. Modbus/ dnp3 state-based intrusion detection system. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pages 729–736, April 2010.
- R. Mitchell and I.-R. Chen. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. Dependable and Secure Computing, IEEE Transactions on, 12(1):16–30, Jan 2015.
- S. Pan, T. Morris, U. Adhikari, Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. IEEE Transactions on Smart Grid, 6(6):3104–3113, 2015.
- R. Berthier, W.H. Sanders, and H. Khurana. Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions. Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, 2010.
- M. Parvania, G. Koutsandria, V. Muthukumary, S. Peisert, C. McParland, and A. Scaglione. Hybrid control network intrusion detection systems for automated power distribution systems. In Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on, pages 774–779, June 2014.

References

- C. Zhou, S. Huang, N. Xiong, et al. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. IEEE Trans. Systems, Man, and Cybernetics: Systems, 45(10):1345–1360, 2015.
- J. Galdun, Dependability Analysis of Networked Control Systems with Consideration of Shared Redundant Subsystems, PhD Kosice-Grenoble, 2008.
- J. Ligušová, JM Thiriet, J. Liguš, P., Barger, Effect of Element Initialization in Synchronous Networked control System to Control Quality, Reliability and Maintainability Annual Symposium, RAMS, p. 135-140, January 2004.
- F-L. Lian, JR Moyne, DM Tilbury, Performance evaluation of control networks: Ethernet, ControlNet,and DeviceNet“, IEEE Control Systems Magazine, Vol. 21, p. 66 – 83, February 2001.
- D. Paret, Le Bus CAN Aplications CAN, CANopen, DeviceNet, OSEK, SDS...“ (in French), ISBN: 2 10 0003659 9, Dunod, Paris, 1999.
- J. Galdun, R. Ghostine, JM Thiriet, J. Liguš, J. Sarnovský,Definition and modelling of the communication architecture for the control of a helicopter-drone, 8th IFAC Symposium on Cost Oriented Automation, Cuba, February 2007
- A. Tanwani, J. Galdun, JM Thiriet, S. Lesecq, S. Gentil, Experimental Networked Embedded Mini Drone - Part I. Consideration of Faults, European Control Conference 2007, Kos, Greece, p.: 4332-4337, ISBN: 978-960-89028-5-5, July 2007.
- L.-B. Fredriksson, A CAN Kingdom – Rev 3.01, KVASER AB, Kinnahult, Sweden, 1995.
- Y. Fourastier, L. Pietre-Cambaceded, Cybersécurité des systèmes industriels, Cepadues, 2015.
- M. Kabir-Querrec, Cyber security of the smart grid control systems: intrusion detection in IEC 61850 communication networks, thèse de Doctorat, Univ. Grenoble Alpes, 2017.
- ISO/IEC 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls, IEC 2013
- ISO/IEC 27005:2018, Information technology -- Security techniques -- Information security risk management, IEC 2018.
- Caselli, M., Zambon, E., and Kargl, F. (2015). Sequence-aware Intrusion Detection in Industrial Control Systems. In *Proc. 1st ACM Workshop CPSS*, pages 13–24.
- Dwyer, M. B., Avrunin, G. S., and Corbett, J. C. (1999). Patterns in property specifications for finite-state verification. In *Proc. ICSE’99*.
- Foulard, C., Flaus, J.-M., and Jacomino, M. *Automatique pour les classes préparatoires : cours et exercices*.
- Lemieux, C., Park, D., and Beschastnikh, I. (2015). General LTL specification mining. In *Proc. ASE’15*, pages 81–92.
- Mitchell, R. and Chen, I.-R. (2014). Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems. *IEEE Tran. on Depend. and Sec. Comp.*, 12(1) :16–30.

References

- Trung Duc TRAN, Jean-Marc THIRIET, Nicolas MARCHAND, Amin El MRABTI. A Cybersecurity Risk Framework for Unmanned Aircraft Systems under Specific Category, Journal of Intelligent and Robotic Systems, Springer Verlag, 2022, 104, pp.4. ⟨10.1007/s10846-021-01512-0⟩
- Stéphane MOCANU, Jean-Marc THIRIET - Real-time performance and security of IEC 61850 process bus communications. Journal of Cyber Security and Mobility, River Publishers, 2021, ⟨10.13052/jcsm2245-1439.1021⟩. ⟨hal-03192264⟩
- Jean-Marc THIRIET, Denis GENON-CATALOT, Stéphane MOCANU, Hamed YAHOUI. Industry 4.0: Educational platforms disseminations in South-East Asia in the field of Automation - EAEEIE 2021 - 30th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE), Sep 2021, Prague, Czech Republic. ⟨10.1109/EAEEIE50507.2021.9530861⟩
- Karem HAFSI, Denis GENON-CATALOT, Jean-Marc THIRIET, Olivier LEFEVRE. DC building management system with IEEE 802.3bt standard, HSPR 2021 IEEE International Conference on High Performance Switching and Routing (HSPR), Jun 2021, Paris, France. pp.1-8, ⟨10.1109/HPSR52026.2021.9481806⟩
- Trung Duc TRAN, Jean-Marc THIRIET, Nicolas MARCHAND, Amin EL MRABTI - Toward Cybersecurity of Unmanned Aircraft System operations under “Specific” category - ICUAS, Athens, 2020, September 1-4, 2020, hal-03108301.
- Stéphane MOCANU, Jean-Marc THIRIET - Experimental study of performance and vulnerabilities of IEC 61850 process bus communications on HSR networks - 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Sep 2020, Genoa, Italy, hal-02921495.
- Jean-Marc THIRIET, Stéphane MOCANU - A course in cyber-security, with orientations towards cyber-physical systems. EAEEIE 2019 - 29th Annual Conference of the European Association for Education in Electrical and Information Engineering, Sep 2019, Ruse, Bulgaria. ⟨hal-02283490⟩
- Trung Duc TRAN, Jean-Marc THIRIET, Nicolas MARCHAND, Amin EL MRABTI, Gabriele LUCULLI - Methodology for risk management related to cyber-security of Unmanned Aircraft Systems - 24th IEEE Conference on Emerging Technologies and Factory Automation (ETFA2019), IEEE Industrial Electronics Society (IES), Sep 2019, Zaragoza, Spain. ⟨hal-02308354⟩
- Jean-Marc THIRIET, Stéphane MOCANU - Some Considerations on Dependability Issues and Cyber-Security of Cyber-Physical Systems - The 7th IEEE International Conference on Smart Communications in Network Technologies (SACONET’18), Oct 2018, El Oued, Algeria, France. 〈hal-01909025〉
- Oualid KOUCHAM, Stéphane MOCANU, Guillaume HIET, Jean-Marc THIRIET, Frédéric MAJORCZYK - Efficient Mining of Temporal Safety Properties for Intrusion Detection in Industrial Control Systems - 10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS'18), Aug 2018, Warsaw, Poland. pp.1-8. ⟨hal-01877109⟩
- Abdelhak MKHIDA, Jean-Marc THIRIET, Jean-François AUBRY - Integration of intelligent sensors in Safety Instrumented Systems (SIS) - Process Safety and Environmental Protection, 92 (2014) 142–149, Elsevier, Elsevier, 2014, 92 (2), pp.142-149 (JCR).
- Faiza CHARFI, Walid LABIDI, Jean Marc THIRIET - Performance Study of a New CSMA/CA Access Method with QoS Based on 802.11b and Comparison with

References

- Zeashan H. KHAN, Jean Marc THIRIET, Denis GENON-CATALOT - Drive-by-Wireless Teleoperation with Network QoS Adaptation – International Journal of Advanced Engineering Sciences and Technologies - ISSN: 2230-7818, Volume 2 Issue 2, février 2011, pp. 160-169.
- Rony GHOSTINE, Jean-Marc THIRIET, Jean-François AUBRY - Variable delays and message losses: influence on the reliability of a control loop - Reliability Engineering & System Safety - RESS-D-09-00489R1, doi:10.1016, Vol 96, Issue 1 (2011) pp. 160-171 (JCR).
- Faiza CHARFI, Oumsaad SLAMA, Jean-Marc THIRIET, Suzanne LESECQ - Improving the control performance in Wireless Network Controlled Systems, using the beacon mode - Journal of telecommunications, Volume 3, Issue 1, June 2010, pp.72-78. ISSN 2042-8839.
- J. M. THIRIET, F. MERIAUDEAU, J. C. BURGUILLO, H. FREMONT, H. YAHOUI, P. de FOOZ - Toward an International Curricula Network for exchanges and LifeLong Learning - Electronics and Electrical Engineering, No. 10 (106), December 2010, pp. 147-150, ISSN 1392-1215.
- J. GALDUN, J.-M. THIRIET, J. LIGUS – Study of different load dependencies among shared redundant systems - Scalable Computing: Practice and Experience, Volume 10, no. 3 (September 2009), Special Issue: Real-Time Distributed Systems and Networks, pp. 241-252, ISSN 1895-1767.
- Zeashan H. KHAN, Denis GENON-CATALOT and J.M. THIRIET - Wireless Network Architecture for Diagnosis and Monitoring Applications - MJC, MASAUM Journal of Computing (ISSN 2076-0833), Volume: 1 Issue: 2, September 2009, pp. 318-325.
- Insaf SASSI, Alexia GOUIN, Jean-Marc THIRIET - Wireless Network Performance Evaluation for Networked Robots - 22nd IEEE International Conference on Emerging Technologies And Factory Automation - ETFA 2017, Sep 2017, Limassol, Cyprus. ⟨hal-01665237⟩
- Insaf SASSI, Alexia GOUIN, Jean-Marc THIRIET - Distributed to Embedded Bayesian Network for Diagnosis of a Networked Robot - IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA 2017), Jun 2017, Annecy, France. ⟨hal-01558499⟩
- Insaf SASSI, Alexia GOUIN, Jean-Marc THIRIET - Diagnosis architecture reconfiguration for a networked mobile robot - 27th European Safety and Reliability Conference (ESREL 2017), Jun 2017, Portorož, Slovenia. ⟨ 10.1201/9781315210469-373 ⟩. ⟨hal-01558498⟩
- Oualid KOUCHAM, Stéphane MOCANU, Guillaume HIET, Jean-Marc THIRIET, Frédéric MAJORCZYK - Detecting Process-Aware Attacks in Sequential Control System - 21st Nordic Conference on Secure IT Systems (NordSec 2016), pp.20-36, Nov 2016, Oulu, Finland. <http://nordsec.oulu.fi>. <hal-01361081>

References

- Ahmed ALTAHER, Stéphane MOCANU, Jean-Marc THIRIET - Dependability Optimization of Process-level Protection in an IEC-61850-Based Substation Walls, Revie & Bedford - 26th European Safety and Reliability Conference, Sep 2016, Glasgow, United Kingdom. Tayor & Francis Group, Risk, Reliability and Safety: Innovation Theory and Practices - ESREL 2016, pp.284, 2016. <http://esrel2016.org/>. <hal-01380261>
- Insaf SASSI, Alexia GOUIN, Jean-Marc THIRIET - A Bayesian network for diagnosis of networked mobile robots - European Safety and Reliability Conference 2016, Sep 2016, Glasgow, United Kingdom. <http://esrel2016.org/>. <hal-01375924>
- Maëlle KABIR-QUERREC, Stéphane MOCANU, Jean-Marc THIRIET, Eric SAVARY - A Test bed dedicated to the Study of Vulnerabilities in IEC 61850 Power Utility Automation Networks - Proceedings of IEEE 21th Conference on Emerging Technologies & Factory Automation (ETFA 2016), Berlin, Germany, September 2016, 2016, <http://www.etfa2016.org/index.php>. <hal-01366270>
- Ahmed ALTAHER, Stéphane MOCANU, Jean-Marc THIRIET - Evaluation of Time-Critical Communications for IEC 61850-Substation Network Architecture - Surveillance 8 International Conference, Oct 2015, Roanne, France. Proceeding of Surveillance 8 2015, <http://surveillance8.sciencesconf.org/>
- Ayoub SOURY, Melek CHARFI, Denis GENON-CATALOT, Jean-Marc THIRIET - Performance analysis of Ethernet Powerlink protocol: Application to a new lift system generation - 20th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA'2015, IEEE, 8-11/9/2015, <10.1109/ETFA.2015.7301492>. <hal-01233841>
- Maëlle KABIR-QUERREC, Stéphane MOCANU, Jean-Marc THIRIET, Eric SAVARY - Power Utility Automation Cybersecurity: IEC 61850 Specification of an Intrusion Detection Function - ESREL 2015, Zurich, 7-10 Septembre 2015.
- Ayoub SOURY, Denis GENON-CATALOT, Jean-Marc THIRIET - New lift safety architecture to meet PESSRAL requirements - 2nd World Symposium on Web Applications and Networking (WSWAN), IEEE Computer Society, 21st to 23rd March 20152015, IEEE, 2015, <10.1109/WSWAN.2015.7210314>. <hal-01233766>

Some references

- J.F. Aubry, Nicolae Brinzei – Systems Dependability Assessment, Modeling with Graphs and Finite State Automata, Wiley, Fév. 2015.
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – *Sûreté de fonctionnement des systèmes industriels* – Editions Eyrolles, Paris, 1988.
- C. Davis, M. Schiller, K. Wheeler - *IT Auditing: using control to protect assets* – 2007, Mc Graw Hill
- Cours Stéphane Mocanu, ENSE3, Industrial Communication Labs, 2016
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Patrick Monassier, cours CESI 2009, Informatique industrielle.
- Pierre Bonnet, cours Université de Lille, Introduction à la supervision, 2010
- EPFL, Industrial Automation course
- P_RAYMOND_BTS_MAI_Les_API
- Transmissions et réseaux, S. Lohier & D. Présent, Dunod, Paris, 2003.
- Cours Stéphane Mocanu, ENSE3, Industrial Communication Labs, 2016
- Cours Emmanuel Simeu, Polytech Grenoble, Supervision
- Cours de Blaise Conrard, Polytech Lille.
- Patrick Monassier, cours CESI 2009, Informatique industrielle.
- Pierre Bonnet, cours Université de Lille, Introduction à la supervision, 2010
- G. Boujat et P. Annaya, Automatique industrielle en 20 fiches, Dunod, 2007
- W. Bolton, Automates programmables industriels, Dunod, 2015.
- Duc Tran Trung , Cybersecurity risk assessment for Unmanned Aircraft System, PhD, Univ. Grenoble Alpes, Feb. 2021

Some references

https://www.technologuepro.com/cours-automate-programmable-industriel/Les-automates-programmables-industriels-API.htm

http://www.est-usmba.ac.ma/coursenligne/GE-S2-M8.1-Automatismes%20logiques%20Industriels-CRS-El%20Hammoumi.pdf

http://colasapoil.free.fr/HEI/HEI5%20TC/Maintenance/h5_tc_maintenance_coursv2_coursv2_1783.pdf

https://www.cours-gratuit.com/cours-divers/cours-sur-les-definitions-methodes-et-operations-de-la-maintenance

https://www.manager-go.com/logistique/organisation-de-la-logistique.htm

https://www.lecoindesentrepreneurs.fr/logistique-entreprise/
https://d1n7iqsz6ob2ad.cloudfront.net/document/pdf/5346e085efe6e.pdf

https://www.icours.com/cours/economie/la-production

https://perso.imt-mines-albi.fr/~fontanil/THESE/5_Partie1_p13_43.pdf

ขอบคุณมากสำหรับความสนใจของคุณ (TH)

Merci pour votre attention

Thank you for your attention

jean-marc.thiriet@univ-grenoble-alpes.fr